

# REGIONAL INFORMATION SHARING SYSTEMS<sup>®</sup> (RISS) PROGRAM

*A Proven Resource for Law Enforcement*



## *Frequently Asked Questions*

1. What is RISS?
2. Where are the six RISS Centers located, and what regions do they serve?
3. How do I contact a RISS Center?
4. What services does RISS provide to its member agencies?
5. What resources are available via the RISS Secure Cloud (RISSNET<sup>™</sup>)?
6. How is RISS different from other nationwide information sharing programs?
7. How is RISS funded?
8. Who governs RISS, and what is the role of the RISS National Policy Group?
9. What is the role of the RISS National Coordinator?
10. What is the role of the RISS Technology Support Center?
11. What is the role of the Institute for Intergovernmental Research<sup>®</sup>?
12. Who are the primary users of RISS?
13. What is RISSNET?
14. What partner agencies are connected to RISSNET?
15. How does an authorized user access RISSNET?
16. What is the RISSNET Portal?
17. What security measures are in place to ensure that information transmissions are secure when using RISSNET?
18. What is the U.S. Department of Justice Global Justice Extensible Markup Language (XML)?
19. What is LEXS?
20. Does RISS consider privacy rights?
21. What is RISSIntel<sup>™</sup>?
22. Are RISS criminal intelligence databases subject to 28 Code of Federal Regulations (CFR) Part 23?
23. What is RISSLinks<sup>™</sup>?
24. What is the RISSLeads Investigative Website<sup>™</sup>?
25. What is RISS ATIX<sup>™</sup>?
26. What is the RISSGang<sup>™</sup> Program?
27. What is RISSafe<sup>™</sup>?
28. What is the RISS Officer Safety Website?
29. What are the RISS Law Enforcement Websites Hosted on RISSNET?
30. How has RISS partnered with fusion centers?
31. How does RISS make use of Federated Identity Management?
32. What is the National Information Exchange Model (NIEM)?
33. How does RISS measure the effectiveness of the program?

## 1. What is RISS?

RISS is a proven, trusted, and innovative program that supports local, state, federal, and tribal criminal justice and public safety agencies in their effort to successfully resolve criminal investigations and ensure officer safety. RISS consists of six regional centers and the RISS Technology Support Center (RTSC). RISS supports efforts against organized and violent crime, gang activity, drug activity, human trafficking, identity theft, and other regional priorities, while promoting officer safety. RISS offers law enforcement agencies and officers full-service delivery, from the beginning of an investigation to the ultimate prosecution and conviction of criminals. An officer can query multiple intelligence databases, retrieve information from investigative systems, solicit assistance from research staff, utilize surveillance equipment, receive training, and use analytical resources to help investigate and prosecute criminals. For more information about RISS, visit [www.riss.net](http://www.riss.net) or find RISS at [www.facebook.com/TheRISSProgram](https://www.facebook.com/TheRISSProgram). Make sure to “like” the page to get updates and information about RISS. Shared successes by state can be viewed at the RISS Impact Website ([www.riss.net/Impact](http://www.riss.net/Impact)).

## 2. Where are the six RISS Centers located, and what regions do they serve?



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



***Mid-States Organized Crime Information Center® (MOCIC)—Springfield, Missouri***—Provides services to Illinois, Iowa, Kansas, Minnesota, Missouri, Nebraska, North Dakota, South Dakota, and Wisconsin, as well as parts of Canada.



***New England State Police Information Network® (NESPIN)—Franklin, Massachusetts***—Provides services to Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, and Vermont, as well as parts of Canada.



***Rocky Mountain Information Network® (RMIN)—Phoenix, Arizona***—Provides services to Arizona, Colorado, Idaho, Montana, Nevada, New Mexico, Utah, and Wyoming, as well as parts of Canada.



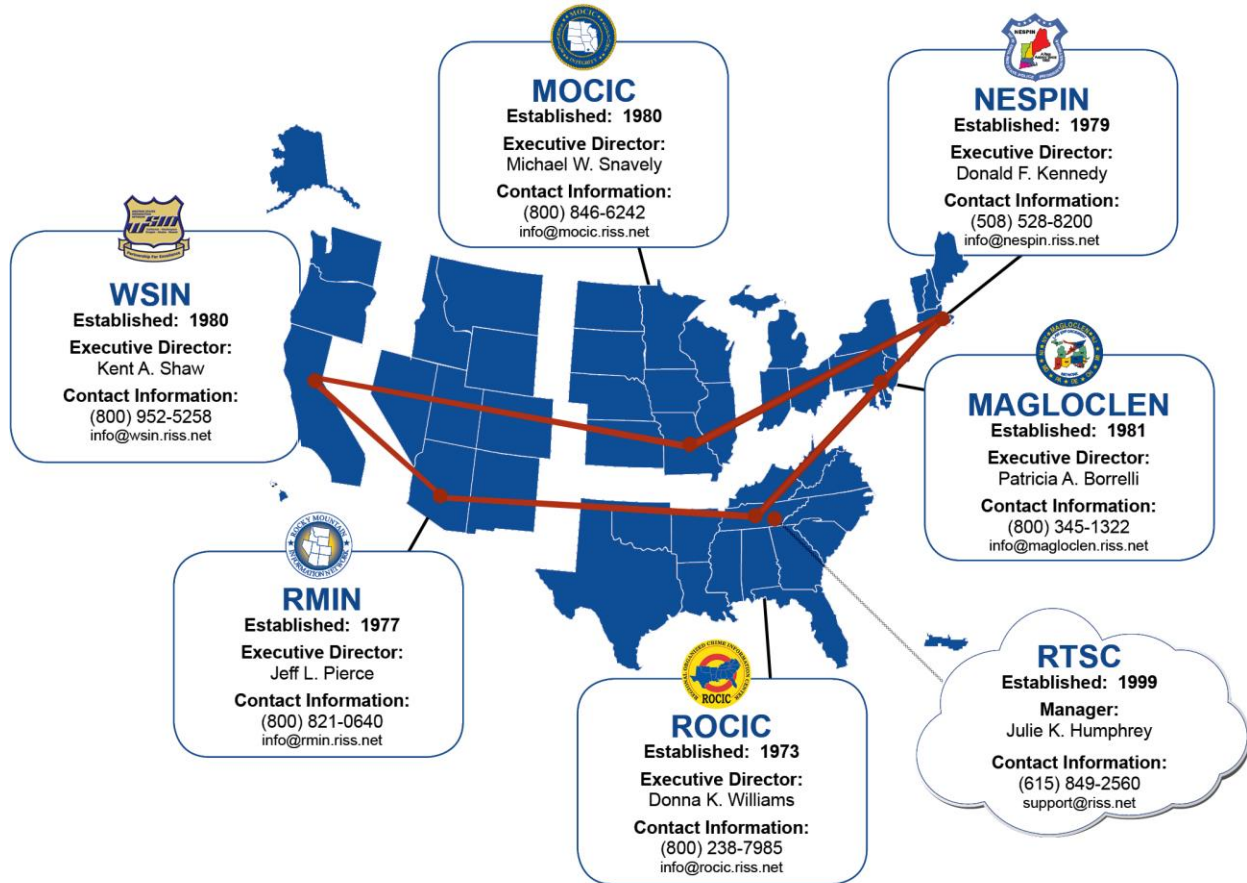
***Regional Organized Crime Information Center® (ROCIC)—Nashville, Tennessee***—Provides services to Alabama, Arkansas, Florida, Georgia, Kentucky, Louisiana, Mississippi, North Carolina, Oklahoma, South Carolina, Tennessee, Texas, Virginia, and West Virginia, as well as Puerto Rico and the U.S. Virgin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



**Western States Information Network® (WSIN)—Sacramento, California—** Provides services to Alaska, California, Hawaii, Oregon, and Washington, as well as Guam, New Zealand, and parts of Canada.

### 3. How do I contact a RISS Center?

Visit [www.riss.net](http://www.riss.net) for additional information.



### 4. What services does RISS provide to its [member agencies](#)?

RISS provides services to support law enforcement member-agency investigations and prosecutions. RISS services include:

- Information sharing through the RISS Secure Cloud (RISSNET™)
- Officer safety and event deconfliction
- Investigative support and research
- Analysis of criminal activity data and development of diverse and varied analytical reports, charts, and diagrams

- Computer/mobile device forensics
- Audio/video enhancements
- Loan of specialized investigative equipment
- Specialized training, conferences, and meetings
- Publications, bulletins, and educational materials
- Field services support and technical assistance

*(Note: Not all services are provided by each RISS Center.)*

## **5. What resources are available via the RISS Secure Cloud (RISSNET™)?**

Examples of the resources developed and/or available via RISSNET to authorized users include:

- RISS Criminal Intelligence Database (RISSIntel™)
- RISS Officer Safety Event Deconfliction System (RISSafe™)
- RISS Officer Safety Website
- RISSGang Program (RISSGang™)
- RISS Automated Trusted Information Exchange™ (ATIX)
- RISSLinks™
- RISSLeads Investigative Website™
- RISS Money Counter Project (MCP)
- RISS Master Telephone Index (MTI)
- Law Enforcement Websites Hosted on RISSNET
- RISS Property and Recovery Tracking System (RISSProp)
- Secure e-mail
- Cold Case Locator System
- National Criminal Intelligence Resource Center (NCIRC)
- National Motor Vehicle Title Information System (NMVTIS)
- Federal Law Enforcement Training Centers' Online Campus (e-FLETC)

## **6. How is RISS different from other nationwide information sharing programs?**

RISS has unique roles and responsibilities; distinctive operational capabilities; multiple sources, formats, and mechanisms to collect and disseminate information; and different users than other criminal justice programs. RISS is the only system built *by* law enforcement *for* law enforcement and is governed by state and local law enforcement.

Systems such as the U.S. Department of Homeland Security's (DHS) Homeland Security Information Network (HSIN), the Federal Bureau of Investigation's (FBI) Law Enforcement Enterprise Portal (LEEP), the National Security Agency's (NSA) Intelink-U, and RISS represent critical components of the Information Sharing Environment ([www.ise.gov](http://www.ise.gov)) and offer valuable services for their individual users. These systems play a unique yet complementary role to help protect our nation by serving as valuable conduits for information sharing among federal, state, local, tribal, and territorial agencies. Each system provides primary services or programs that make it distinct.

Examples of the distinctive criminal justice and officer safety resources provided by RISS through RISSNET include:

- [RISSIntel](#)
- [RISSLeads Investigative Website](#)
- [RISS ATIX](#)
- [RISSGang](#)
- [RISSafe](#)
- [RISS Officer Safety Website](#)
- RISSProp
- RISS MCP
- RISS MTI
- Law Enforcement Websites Hosted on RISSNET

RISS works closely with many partners, including HSIN, LEEP, and Intelink-U, to provide criminal justice and homeland security agents at all levels of government with secure, easy access to critical information from multiple partner systems. RISS and its partners share information securely using two complementary approaches: (1) single sign-on using [federated identity technology](#) and (2) system-to-system information sharing.

RISS also provides critical officer safety event deconfliction through RISSafe and maintains the RISS Officer Safety Website.

In addition to automated capabilities, RISS provides investigative support, such as analytical services, equipment loans, technical assistance, case funds support, training and publications, and intelligence research.

## **7. How is RISS funded?**

RISS is congressionally funded and administered by the [U.S. Department of Justice \(DOJ\), Office of Justice Programs \(OJP\), Bureau of Justice Assistance \(BJA\)](#), through grant awards. BJA provides funding oversight and program management for the RISS Program.

It is important to note that although RISS is congressionally funded, it is locally managed. See [“Who governs RISS, and what is the role of the RISS National Policy Group?”](#) for more information.

## **8. Who governs RISS, and what is the role of the RISS National Policy Group?**

RISS is governed by its local and regional member law enforcement agencies through individual RISS Center policy boards. The RISS National Policy Group (RNPG) is composed of the six RISS Center Directors and the chair of each RISS Center’s policy board or his or her designee. Each RISS Center has an established policy board or executive committee composed of representatives from member criminal justice agencies in the center’s multistate region. The primary purpose of center policy boards is to provide direction affecting center policy, operation, and administration.

The RNPG is responsible for strategic planning, resolution of operational issues, advancement of information sharing, and decision making affecting the RISS Centers, the nationwide organization, service delivery, member agencies, and related partner organizations.

**9. What is the role of the RISS National Coordinator?**

The RISS National Coordinator represents RISS at the nationwide level, ensures optimal communication and coordination efforts with RISS partners, and fosters opportunities to present RISS solutions for information sharing, deconfliction, and investigative support.

**10. What is the role of the RISS Technology Support Center?**

The RISS Technology Support Center (RTSC) Manager oversees the operations of the RTSC, which consists of the Applications Development Group and the Intranet Operations Group. The RTSC staff develops and maintains technical programs and projects that provide critical information services to RISS and its information sharing partners. The RTSC also maintains RISSNET and supports the RISS Centers in their information technology efforts.

**11. What is the role of the Institute for Intergovernmental Research®?**

The Institute for Intergovernmental Research (IIR) is a Florida-based nonprofit research and training organization specializing in law enforcement, juvenile justice, and criminal justice issues. IIR serves as the technical service provider for ongoing technical training, research, and analysis services to the RISS Program through the support of grant awards received from BJA. IIR supports RISS by providing project coordination activities, policy development assistance, research and program planning, performance measurement and evaluation, meeting coordination, training, and information systems support. IIR provides for management support and spending related to the operation of RISSNET and RISS database applications, including liaison to RISS information technology operational and applications development components, coordination of information technology support, and processing of technology purchases and acquisitions. IIR has worked with the RISS Program for more than 30 years providing technical assistance support services. For more information about IIR, visit [www.iir.com](http://www.iir.com).

**12. Who are the primary users of RISS?**

The primary users of RISS and RISSNET are local, state, federal, and tribal law enforcement member-agency personnel. RISS supports the investigative and prosecution efforts of member agencies in all 50 states, the District of Columbia, U.S. territories, Canada, England, and New Zealand. RISS also provides services and tools to thousands of public safety and private sector partners through the [RISS ATIX](#) program.

RISS membership has grown to more than 9,000 law enforcement and criminal justice agencies, including more than 141,000 authorized users.

Agency membership is required for access to most RISS resources (some exceptions include RISSafe, RISSGang, and RISS ATIX). Membership is a critical component to ensuring a trusted

network of users as well as the integrity of the overall information sharing process and RISSNET and its related programs and applications.

Each RISS Center has implemented a membership application and policy board approval process. Agency membership is typically open to all local, state, federal, and tribal law enforcement agencies; prosecution agencies; and corrections agencies, as well as multijurisdictional task forces and regulatory agencies with law enforcement or criminal investigative authority. **However, it is important to note that membership in a RISS Center is governed by the specific RISS Center's rules, procedures, policies, constitution, and/or bylaws.**

Law enforcement agencies may access RISSafe, the RISS Officer Safety Website, RISSGang, and other resources—after completing a thorough vetting process—without the requirement to establish RISS membership. In addition, individuals participating in RISS ATIX also complete a vetting and approval process prior to accessing ATIX resources.

RISS has established information sharing partnerships with member and nonmember law enforcement agencies at the state and federal levels based on federated identity technology. RISS's federated partnerships provide its members with access to numerous information services that are available on partner systems and provide users of partner systems with access to resources on RISSNET.

### **13. What is RISSNET?**

RISSNET is a secure sensitive but unclassified (SBU) law enforcement information sharing cloud provider. RISSNET provides access to millions of pieces of data, offers system-to-system sharing of information, and connects disparate state, local, and federal systems. Agencies can easily connect to RISSNET, share information and intelligence in a secure environment, and query multiple systems simultaneously. Currently, more than 80 systems are connected or pending connection to RISSNET. In addition, there are hundreds of resources available via RISSNET to authorized users; the owners of these resources rely on RISSNET for its secure infrastructure. RISSNET enables users to connect quickly using secure web-based technologies at both National Institute of Standards and Technology (NIST) Level 2 and NIST Level 3.

Through information sharing partnerships based on federated identity technology, RISSNET provides users of partner systems with secure access to RISSNET resources and enables RISS members to access resources provided by federal agencies, such as the FBI's Joint Automated Booking System (JABS), the NSA Intelink-U Website, the FBI's National Data Exchange (N-DEx), and the FLETC Online Campus, to name a few.

### **14. What partner agencies are connected to RISSNET?**

Currently, more than 80 partner agencies are connected or pending connection to RISSNET. RISSNET serves state law enforcement systems, High Intensity Drug Trafficking Areas (HIDTA) network systems, fusion centers, and federal and other systems electronically connected to RISSNET. Examples of connected systems include:

- Arizona Department of Public Safety
- Boston Regional Information Center
- Bureau of Alcohol, Tobacco, Firearms and Explosives
- California Department of Justice, Bureau of Investigation/Association of Law Enforcement Intelligence Units
- Cincinnati/Hamilton County Terrorism Early Warning Group
- Colorado Bureau of Investigation
- Connecticut Intelligence Center
- Delaware Statewide Intelligence System
- El Paso Intelligence Center (EPIC)
- Indiana Intelligence Fusion Center
- INTERPOL
- Iowa Department of Public Safety Intel/Law Enforcement Intelligence Network
- Kansas Intelligence System
- Maryland Coordination and Analysis Center
- Massachusetts CrimeNTel
- Montana Division of Criminal Intelligence
- National Gang Intelligence Center
- NSA Intelink-U
- National Virtual Pointer System (NVPS)
- Nebraska Fusion Center
- New Jersey Statewide Intelligence System
- New York State Intelligence Center
- Nlets—The International Justice and Public Safety Network
- Ohio Bureau of Criminal Investigation
- Ohio Department of Public Safety
- Pennsylvania State Police
- Philadelphia Police Department
- Rhode Island State Police
- U.S. Department of Justice, Criminal Division
- United States Postal Inspection Service
- United States Secret Service, National Threat Assessment Center
- Vermont Intelligence Center
- Washington State Gang Database (WAGang)

**15. How does an authorized user access RISSNET?**

For staffs of member agencies, access to RISSNET can be achieved through a single computer connection using an Internet Service Provider (ISP) or via a RISSNET connection of an agency information technology system. Member-agency staff may contact their in-region RISS Center to request access. To find out how to connect to RISSNET, contact your in-region RISS Center. For RISS Center contact information, click [here](#).



Users of partner systems that use federated identity technology to access RISSNET are eligible to access certain resources on RISSNET. These federated partner systems provide their users with a link to the RISSNET Portal. If the user has already logged on to the user's home system, the user will be connected to RISSNET without requiring a second log-on. If the user of the partner system reached the RISSNET Portal without having logged on to the user's home system, the user will be redirected to the user's home system to complete the log-on process. Contact your system administrator or Help Desk to learn whether your system has a federated partnership with RISS.

**16. What is the RISSNET Portal?**

The RISSNET Portal provides users with a streamlined log-on process, ease of access to resources available on RISSNET, and enhanced search capabilities to RISSNET and partner resources.

**17. What security measures are in place to ensure that information transmissions are secure when using RISSNET?**

The technical capabilities and systems architecture implemented by RISS permit authorized users to interact electronically with one another in a secure environment. RISSNET protects these transmissions through the use of encryption, user authentication, Internet Protocol security standards, and firewalls to prevent unauthorized access.

**18. What is the U.S. Department of Justice Global Justice Extensible Markup Language (XML)?**

RISS has numerous connections with partner systems using XML—a worldwide technology standard—to communicate criminal intelligence information. Soon after the initial publication of the XML standard, RISS developed in-house XML formats for data exchange. In conjunction with other early practitioners of XML in the criminal justice community, RISS has been actively involved with the Global Justice Information Sharing Initiative (Global) to develop standards for the community, including the Global Reconciliation Data Dictionary (RDD), the Global Justice XML Data Model (GJXDM), the National Information Exchange Model (NIEM), and the Logical Entity eXchange Specifications (LEXS). For more information on Global and XML, visit [www.it.ojp.gov](http://www.it.ojp.gov).

**19. What is LEXS?**

LEXS is a NIEM-based framework for the development of information exchanges. Initially developed for the law enforcement information sharing program at DOJ, LEXS is now being widely used in the criminal justice community at large, as well as by the homeland security, intelligence, and other communities. RISS utilizes a LEXS-based connection to many law enforcement agencies for the exchange of criminal intelligence and is an active participant on the LEXS Planning Committee.

**20. Does RISS consider privacy rights?**

RISS recognizes the need to ensure that an individual's constitutional rights, civil liberties, civil rights, and privacy interests are protected throughout the intelligence process. RISS has adopted a privacy policy that complies with 28 CFR Part 23 and is based on the Global privacy guidelines. All RISS member agencies agree to comply with the requirements of 28 CFR Part 23 with respect to any criminal information they submit into applicable RISS criminal intelligence databases. RISS encourages all law enforcement agencies to voluntarily adopt appropriate and clearly defined privacy and security safeguards for all agency intelligence missions to manage and control collection, retention, and dissemination activities. To access the RISS Privacy Policy, visit [www.riss.net/privacy.aspx](http://www.riss.net/privacy.aspx).

**21. What is RISSIntel™?**

RISSIntel is a web-based application that provides for real-time, online federated searches of RISS and partner intelligence databases, including state intelligence systems, fusion centers, and systems connected via NVPS. RISSIntel permits federated searching across many systems without requiring the RISSNET user to have a separate user account for each partner system. Member-agency personnel may also contact their in-region RISS Center intelligence research staff via telephone, fax, or e-mail for assistance in performing searches.

Millions of records are available via RISSIntel and between connected partner systems. Records include individuals, organizations and gangs, and associates, as well as locations, vehicles, weapons, and telephone numbers. When information is located in any of the connected databases, the user is referred to agencies that have additional information. The databases are designed to encourage exchange of information and coordination among member agencies.

Member agencies are able to submit large volumes of data for inclusion in the databases through software applications implemented by RISS.

One of RISS's primary goals is to provide law enforcement with a conduit for sharing criminal intelligence information. By leveraging the RISSIntel applications, agencies can utilize existing technology through an instance of RISSIntel known as RISS7. Offering this resource provides agencies with a solution without developing new stand-alone systems. Instead, law enforcement agencies can operate and control an autonomous criminal intelligence database while being a part of the broader RISSNET community.

**22. Are RISS criminal intelligence databases subject to 28 Code of Federal Regulations (CFR) Part 23?**

All RISS criminal intelligence databases comply with 28 CFR Part 23, issued by OJP, BJA. All criminal intelligence databases electronically connected to RISSNET that are available for member-agency access must also comply with 28 CFR Part 23. RISS provides member agencies with training and on-site technical assistance to ensure compliance with the regulation. For additional information on 28 CFR Part 23, visit <https://www.iir.com/Documents/28CFR/28cfrpart23overviewbrochure2015.pdf>.

**23. What is RISSLinks™?**

RISSLinks is an online data visualization and analysis capability that enables RISS staff and agency officers to view, in a link chart format, information found in the RISSIntel and RISSGang criminal intelligence databases.

**24. What is the RISSLeads Investigative Website™?**

RISSLeads enables authorized law enforcement officers to search and post information regarding a particular case or other law enforcement issues. Case information is posted with the intent of generating investigative leads. Member agencies share intelligence by viewing and responding to posted information. RISSLeads provides geographically disparate law enforcement professionals with the opportunity to convene electronically to discuss crime trends or specific cases and share investigative techniques. Both open and private information sharing platforms are available.

**25. What is RISS ATIX™?**

RISS ATIX leverages the RISSNET infrastructure to provide a secure platform for law enforcement, public safety, first responders, and the private sector organizations involved in securing our nation from terrorism and other disasters to share information. Community groups include local, county, state, and tribal levels of emergency management, law enforcement, and government, as well as public and private utilities, transportation, agriculture, chemical manufacturing, private security, environmental protection, banking and finance, and hospitality industries.

**26. What is the RISSGang™ Program?**

The RISSGang Program consists of the RISS National Gang Intelligence Database, the RISSGang Website, and informational resources. The database, which is 28 CFR Part 23-compliant, provides law enforcement agencies with access to gang records, including suspects, organizations and gangs, weapons, locations, and vehicles, as well as gang terminology, visual imagery of gang members, gang symbols, gang graffiti, cryptography/codes and hand signs. The website provides a vast amount of resources, information, and publications. In an effort to increase the sharing of gang information, RISS provides access to the RISSGang Program resources to all criminal justice agencies without the requirement to establish RISS membership.

**27. What is RISSafe™?**

RISSafe is an officer safety event deconfliction system. RISSafe stores and maintains data on planned law enforcement events—such as raids, controlled buys, and surveillances—with the goal of identifying and alerting affected agencies and officers of potential conflicts impacting law enforcement efforts. RISSafe is used in conjunction with mapping software to verify data on event locations when an event is entered into the system. If a conflict is identified, immediate notification to the submitting officer occurs, as well as notification to the officers involved by a RISSafe Watch Center. RISSafe makes a significant contribution towards enhancing officer safety and citizen safety and supporting criminal investigations.

RISSafe Mobile enables officers to access RISSafe from the following mobile operating system platforms: iPhone® OS (including the iPad®), Windows Mobile®, and Android™ devices.

The three nationally recognized event deconfliction systems—Case Explorer, RISSafe, and SAFETNet—were connected in May 2015. As of September 2016, the state of New York, including New York City, is not connected to the Nationwide Officer Safety Event Deconfliction System. Work is under way to integrate the primary deconfliction agency in New York—the New York/New Jersey HIDTA. Visit [www.ncirc.gov/deconfliction](http://www.ncirc.gov/deconfliction) for more information.

## **28. What is the RISS Officer Safety Website?**

The RISS Officer Safety Website serves as a nationwide repository for topics related to officer safety, such as concealments, hidden weapons, armed and dangerous threats, officer safety videos, special reports, and training. RISS members and registered users of the VALOR Web Portal who are sworn law enforcement are able to access the RISS Officer Safety Website and vice-versa. Users of federated partner systems who are also designated as sworn law enforcement officers also have access to the RISS Officer Safety Website.

## **29. What are the Law Enforcement Websites Hosted on RISSNET?**

In addition to the many online resources available to RISSNET users, RISS offers its partners the ability to establish secure, full-function collaboration websites on a nationwide, regional, local, or team level. These secure collaboration sites are hosted by RISS on RISSNET, in coordination with the in-region RISS Center, and are available, as approved by the in-region RISS Director, to any RISS law enforcement partner or prospective partner, regardless of RISS membership, who has a legitimate need for this service. Access to the information stored on secure hosted sites is under the control of the partner-assigned website owner.

RISS works with its partners to develop each secure hosted website so that members of the partner's group can share information, post materials, and communicate with each other. There are more than 40 sites housed on RISSNET. Examples of these sites include:

- Federal Law Enforcement Training Accreditation
- Medicaid Fraud Control Units
- Medicaid Integrity Institute
- Vehicle Theft Investigators
- National Interagency Fire Center
- New Jersey Office of Homeland Security and Preparedness
- New Jersey Regional Operations Intelligence Center
- Pennsylvania Criminal Intelligence Center
- Alabama Gang Investigators Association
- Midwest Gang Investigators Association (Kentucky Chapter)

### **30. How has RISS partnered with fusion centers?**

RISS Centers have actively engaged with fusion centers in a variety of ways, including colocating efforts, participating as members of fusion center governance bodies, and partnering with HSIN. In addition, almost all fusion centers have access to RISSNET, thus fostering the collaboration between RISS Centers and fusion centers. RISS intelligence analysts interact daily with staff members at various fusion centers, and in some instances, RISS Center staff members are assigned to a fusion center. Fusion center and RISS staffs benefit from daily interactions that enable them to capitalize on each other's knowledge and experience.

RISS provides technical on-site assistance to fusion centers to integrate RISS services and resources into their daily operations and coordinates the delivery of RISS services with fusion center personnel. RISS also provides the fusion center staff with on-site training, research, and topical publications. Through RISS's sponsored and cosponsored training opportunities, courses such as anti-terrorism, analytical techniques, and 28 CFR Part 23 are made available. RISS researches, drafts, and disseminates publications related to fusion centers and information sharing strategies to thousands of criminal justice professionals.

RISS worked with fusion centers in the Northeast region to connect their intelligence systems via RISSIntel to share critical intelligence information between and among fusion centers. This project, known as the Northeast Fusion Center Intelligence Project, has proved successful, and work continues to expand this effort to other regions.

### **31. How does RISS make use of Federated Identity Management?**

A need existed to enable authorized users from systems outside of RISSNET to access information on RISSNET using a digital credential originating at the user's home system. To provide this access, RISS initiated the Trusted Credential Project, which enabled RISS to create and accept credentials in the form of Security Assertion Markup Language (SAML) and exchange them with other systems.

RISS's early involvement in Federated Identity Management enabled it to participate in two groundbreaking nationwide justice-related information sharing initiatives beginning in 2005: (1) the Global Federated Identity and Privilege Management (GFIPM) Project and (2) the Law Enforcement Information Sharing Program (LEISP) Federated Identity Project.

The GFIPM and LEISP Projects took slightly different approaches and included different participants, but both proved useful to their partners and resulted in the creation of two ongoing identity-based federations that actively connect critical criminal justice and public safety information with authorized users. The GFIPM Demonstration Project resulted in standards and procedures used to create the National Identity Exchange Federation (NIEF), and the LEISP pilot resulted in the establishment of LEEP.

As of December 31, 2016, there were more than 35,000 users from trusted partner systems using Federated Identity Management to access RISSNET resources.

**32. What is the National Information Exchange Model (NIEM)?**

NIEM's mission is to develop a unified strategy, partnerships, and technical implementations for national information sharing by joining together communities of interest. NIEM leverages the data exchange standards efforts successfully implemented by Global and extends the GJXDM to facilitate timely, secure information sharing across the entire justice, public safety, emergency and disaster management, intelligence, and homeland security enterprise. For more information about NIEM, visit [www.niem.gov](http://www.niem.gov).

**33. How does RISS measure the effectiveness of the program?**

RISS has been aggressively setting and achieving performance metrics since its inception. The RISS STatistical Assessment Team (RSTAT), chaired by one of the RISS Directors, is tasked to review the validity, meaningfulness, impact, and trend of all of the measures. The RSTAT and RISS Directors routinely analyze and evaluate performance indicators and discuss findings and observations. RISS reports results for a number of approved performance measures, which are used to evaluate and assess RISS Program effectiveness.

In addition, a RISS Adaptive Strategy combines a traditional strategic plan containing goals, objectives, and performance metrics and applies an ongoing adaptive evaluation process to address rapidly changing environments, security threats, resources, budgets, and changes in technology. RISS reviews its goals and objectives at least annually to determine whether those goals and objectives continue to support the RISS vision and mission.

RISS FAQs August 2017.docx