REGIONAL INFORMATION SHARING SYSTEMS® (RISS) PROGRAM

Privacy Policy

A Proven Resource for Law Enforcement™

August 2013

Contents

Approval Date:	Effective Date:	Revision:
August 6, 2009	August 6, 2009	July 5, 2011 (Ratified July 26, 2011) August 21, 2013

Section 1: Introduction and Purpose Statement

The Regional Information Sharing Systems (RISS) Program was established almost four decades ago, primarily to promote law enforcement information sharing. Information sharing is a critical element in effectively and efficiently detecting, deterring, apprehending, and prosecuting criminals and terrorists. Because of the focused effort by law enforcement and criminal justice agencies from all levels of government, numerous improvements have been made in recent years to ensure that the right individuals receive the right information at the right time. The way law enforcement conducts business today is much different, with technology evolving faster each day. It is vital that the law enforcement community have the capability to instantly communicate and share information. Likewise, law enforcement must also protect, respect, and uphold the privacy, civil rights, and civil liberties of individuals.

RISS supports law enforcement and public safety efforts in a variety of ways, including information sharing, investigative research assistance, analytical support, technical equipment loans, confidential funds, training, publications development and dissemination, field services, and technical assistance.

The intent of this RISS Privacy Policy is to protect individual privacy, civil rights, civil liberties, and other protected interests and to address the proper handling of:

- Personally identifiable information (PII) housed in resources maintained and operated by the RISS Program, such as the RISS Criminal Intelligence Databases (RISSIntel™);
- Other criminal justice information available to authorized RISS Center staff, such as criminal history information, suspicious activity reporting (SAR) information, and other investigative information; and
- Personally identifiable information that member agencies, individual officers, analysts, participants, partners, and other entities provide to RISS in order to become a RISS member or participant and to access RISS-related resources and services.

This privacy policy was developed in accordance with the Global Justice Information Sharing Initiative (Global) *State and Local Privacy Policy Development Template: Privacy, Civil Rights, and Civil Liberties Policy Workbook*. In addition, supporting documents, such as the *Fusion Center Privacy Policy Development* document, were reviewed and used, as appropriate. RISS also consulted privacy experts during the development of this policy.

Section 2: Definitions

A. Authorized User—an individual who has successfully completed the RISS identification and approval process or who is accessing RISS resources through an established federated identity partnership and has been granted permissions to appropriate information technology resources available via RISS.
B. Electronic Communication—any communication that is broadcast, created, sent, forwarded, replied to, transmitted, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several electronic systems, devices, or services.

C. Fusion Center—a collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity. (Source: *Fusion Center Guidelines*)

D. Homeland Security Information—as defined in Section 892(f)(1) of the Homeland Security Act of 2002 and codified at 6 U.S.C. § 482(f)(1), homeland security information means any information possessed by a federal, state, or local agency that:
   1. Relates to a threat of terrorist activity;
   2. Relates to the ability to prevent, interdict, or disrupt terrorist activity;
   3. Would improve the identification or investigation of a suspected terrorist or terrorist organization; or
   4. Would improve the response to a terrorist act.

E. Information Sharing Environment (ISE) Suspicious Activity Report (SAR) (ISE-SAR)—a suspicious activity report (SAR) that has been determined, pursuant to a two-step process established in the ISE-SAR Functional Standard, to have a potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism). See also Suspicious Activity and Suspicious Activity Report (SAR).

F. Law Enforcement Investigative Purpose—the situation in which data can be directly linked to a criminal justice or law enforcement agency's authorized investigative activity.

G. Need to Know—as a result of jurisdictional, organizational, or operational necessities, access to sensitive information or intelligence is necessary for the conduct of an individual's official duties as part of an organization that has a right to know the information in the performance of a law enforcement, homeland security, or counterterrorism activity, such as to further an investigation or meet another law enforcement requirement.

H. Participating Agency(ies)—any vetted or approved law enforcement, criminal justice, or public safety entity and private partners utilizing RISS's services, resources, and network. This includes those individuals vetted as ATIX Participants, member agencies, and other partners.

I. Personally Identifiable Information—one or more pieces of information that, when considered together or when considered in the context of how they are presented or how they are gathered, are sufficient to specify a unique individual. The pieces of information include:
   1. Personal characteristics such as height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation, place of birth, mother's maiden name, distinguishing features, and biometric information such as fingerprints, DNA, and retinal scans.
   2. A unique set of numbers or characters assigned to a specific individual, including name, address, phone number, social security number, e-mail address, driver's license number, financial account, or credit card number and associated PIN number, Integrated Automated Fingerprint Identification System (IAFIS) identifier, or booking or detention system number.
   3. Descriptions of events or points in time, including information in documents such as police reports, arrest reports, and medical records.
   4. Descriptions of locations or places, including geographic information systems (GIS) locations, electronic bracelet monitoring information, etc.

J. Right to Know—based on having legal authority or responsibility or pursuant to an authorized agreement, an agency or organization is authorized to access sensitive information and intelligence in the performance of a law enforcement, homeland security, or counterterrorism activity.

K. RISS ATIX™ Participant—executive and official staff from governmental or nongovernmental entities involved with planning and implementing prevention, response, mitigation, and recovery efforts regarding terrorism, disasters, or other law enforcement and public safety strategic and tactical response efforts who have successfully completed the RISS identification and approval process for access to RISS ATIX resources.

L. RISS Member Agency—a criminal justice or law enforcement agency or organization approved for membership by a RISS Center policy board and provided access to appropriate RISS services and resources.

M. RISS Secure Cloud (RISSNET™)—RISSNET is a secure sensitive but unclassified (SBU) law enforcement information sharing cloud provider. RISSNET serves as a secure communications backbone and infrastructure for sharing criminal intelligence and other law enforcement and public safety-related information. RISSNET provides a secure platform at the SBU level for communications among agencies, as well as access to various state and federal criminal intelligence and information systems across the country.

N. RISSNET Node/Node Partner—any local area network (LAN) or wide area network (WAN) electronically connected to RISSNET infrastructure via (1) a dedicated communications circuit and a RISSNET-compliant firewall or (2) an Internet Protocol Security/Virtual Private Network (IPsec VPN) connection and a RISSNET-compliant router.

O. Suspicious Activity—observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity. (Source: ISE-SAR Functional Standard (Version 1.5)) Examples of suspicious activity with a potential nexus to terrorism include surveillance, photography of sensitive infrastructure facilities, site breach or physical intrusion, cyberattacks, testing of security, etc.

P. Suspicious Activity Report (SAR)—official documentation of observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity. SAR information offers a standardized means for supplying information repositories or data analysis tools. Patterns identified during SAR information analysis may be investigated in coordination with the reporting agency and, if applicable, a state or regional fusion center. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor is it designed to support interagency calls for service.

Q. Terrorism Information—consistent with Section 1016(a)(5) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), all information relating to (a) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or materials support, or activities of foreign or international terrorist groups or individuals or of domestic groups or individuals involved in transnational terrorism; (b) threats posed by such groups or individuals to the United States, United States persons, or United States interests or to those interests of other nations; (c) communications of or by such groups or individuals; or (d) other groups or individuals reasonably believed to be assisting or associated with such groups or individuals. Weapons of Mass Destruction (WMD) information was defined and included in the definition of "terrorism information" by P.L. 110-53.

R. Terrorism-Related Information—in accordance with the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended by the 9/11 Commission Act (August 3, 2007, P.L. 110-53), the Office of the Program Manager, Information Sharing Environment (PM-ISE), facilitates the sharing of terrorism and homeland security information, as defined, respectively, in IRTPA Section 1016(a)(5) and the Homeland Security Act 892(f)(1) (6 U.S.C. § 482(f)(1)). See also Information Sharing Environment Implementation Plan (November 2006) and Presidential Guidelines 2 and 3 (the ISE will facilitate the sharing of "terrorism information," as

defined in the IRTPA, as well as the following categories of information to the extent that they do not otherwise constitute "terrorism information": (1) homeland security information as defined in Section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. § 482(f)(1)) and (2) law enforcement information relating to terrorism or the security of our homeland). Such additional information may include criminal intelligence information.

Section 3: Governance and Oversight

RISS is a congressionally funded program administered by the U.S. Department of Justice (DOJ), Office of Justice Programs (OJP), Bureau of Justice Assistance (BJA).

The RISS National Policy Group (RNPG) is composed of the six RISS Center Directors and the chair of each RISS Center's policy board. The RISS Center's policy board (or executive committee) is established by each RISS Center and composed of representatives from member criminal justice agencies in the center's geographic service area. The primary purpose of the board is to provide direction affecting center policy, operation, and administration.

The primary purpose of the RNPG is to provide direction affecting RISS Center policies, operations, and administration. The RNPG is responsible for strategic planning, resolution of operational issues, advancement of information sharing, and other matters affecting the RISS Program and RISS Centers. Each of the RISS Directors, individually and collectively, is responsible for the overall operation of the RISS Program, including its justice information systems, information collection and retention procedures, coordination of personnel, and enforcement of this policy.

Section 4: RISS Owned and Operated Information Technology Resources

RISS has developed and continues to maintain and operate a number of intelligence and investigative resources to assist and support law enforcement and public safety entities. The following resources include electronic systems or databases available to authorized users via RISSNET:

- RISS Criminal Intelligence Databases (**RISSIntel**), as well as various state, regional, federal, and specialized criminal justice information systems. (Note: While RISS operates RISSIntel, RISS does not maintain or operate these individual state, regional, federal, and specialized criminal justice information systems.)
- The 7th Instance of the RISS Suite of Applications (RISSApps), known as **RISS7**—an alternate criminal intelligence database for deployment and use in law enforcement agencies to store collected criminal intelligence data.
- RISS National Gang Program (**RISSGang**™)—consists of a gang-related criminal intelligence database, secure communications tools, and a secure website.
- RISS Automated Trusted Information Exchange™ (**RISS ATIX**)—includes secure web pages, a discussion forum, a document library, and secure e-mail for law enforcement and public safety entities.
- RISS Officer Safety Event Deconfliction System (**RISSafe**™)—stores and maintains data on planned law enforcement events with the goal of identifying and alerting affected law enforcement agencies to potential conflicts with other law enforcement agencies' events.

- RISS Officer Safety Website—serves as a national repository for officer safety information and resources, including concealments, hidden weapons, armed and dangerous threats, officer safety videos, special reports, and training opportunities.
- RISSLeads Investigative Website™—provides a secure electronic bulletin board that enables users to post information on a case or raise or respond to other law enforcement issues.
- Data Visualization and Link Analysis Tool (**RISSLinks**™)—provides an analytical chart when a record is viewed by a user in RISSIntel that visually depicts the associations between people, places, and things.
- Other resources include the RISS search engine (**RISSearch**), individual RISS Center websites, and secure e-mail.
- Other information technology resources operated by individual RISS Centers, such as investigative databases.

A. 28 Code of Federal Regulations (CFR) Part 23 Compliance

1. RISS firmly recognizes the need to ensure that individuals' privacy, other civil liberties, and civil rights are protected throughout the intelligence and information sharing process.
2. RISS endorses the *National Criminal Intelligence Sharing Plan's* (NCISP) guideline that ensures that "the collection, submission, access, storage, and dissemination of criminal intelligence information conforms to the privacy and constitutional rights of individuals, groups, and organizations" and that "law enforcement agencies shall adopt, at a minimum, the standards required by the Criminal Intelligence Systems Operating Policies federal regulation (28 CFR Part 23)."
3. RISS Centers have adopted policy guidelines that fully comply with 28 CFR Part 23. All RISS member agencies have also agreed, in writing, to comply with the requirements of 28 CFR Part 23 with respect to any criminal intelligence information they submit into or receive from applicable RISS criminal intelligence databases.
4. RISS criminal intelligence databases are maintained in compliance with 28 CFR Part 23. This includes requirements governing receipt, storage, and maintenance of criminal intelligence information; exclusion of illegally obtained information; restrictions on dissemination; observance of administrative, technical, and physical safeguards (including establishment of audit trails); review and purge requirements; and forbidding the purchase or use of any electronic, mechanical, or other device for surveillance that is in violation of the provisions of the Electronic Communications Privacy Act of 1986 or applicable state law related to wiretapping or surveillance.

B. Policy Applicability and Legal Compliance

1. **RISS Staff—**RISS staff will be provided a printed or electronic copy of this policy. Staff will acknowledge receipt of this policy by e-mail notification or other appropriate method. By acknowledging receipt of this policy, staff members agree to comply with this policy and with applicable laws and regulations protecting privacy, civil rights, and civil liberties.
2. **Partners/Contractors/Others—**RISS participating agencies, users, partners, contractors, and others, as appropriate, will be governed by participation applications, user agreements, and contracts, which will comply with the provisions of this policy and with applicable laws protecting privacy, civil rights, and civil liberties. Relevant portions of this policy will be

included in agreements and contracts. Agreements and contracts will reference the full policy and its location.

3. A copy of the RISS Privacy Policy will be made available upon request. The latest version of this policy will be posted at the RISS public website, www.riss.net.

C. New Information Technology Initiatives

1. The RNPG or individual RISS Centers may partner with other criminal justice entities to enhance information sharing programs or develop new programs and initiatives that further the RISS Program's mission and goals. The RNPG, a RISS Center Director, or the RISS Technology Support Center (RTSC) Manager will conduct, as appropriate, a privacy assessment of new or emerging initiatives. RISS will leverage the Global *Guide to Conducting Privacy Impact Assessments (PIA) for State, Local, and Tribal Information Sharing Initiatives* for this purpose.
2. The PIA will be completed, as appropriate, by the RNPG, the appropriate RISS Center, or a designee and will be maintained by the RNPG, the RISS Center, or a designee.
3. Annually, RISS will adjust, as required, the project strategy, technology specifications, this privacy policy, and/or other appropriate operating policies and procedures to ensure that privacy, civil rights, and civil liberties are protected in the implementation of a new or expanded information sharing program or initiative.

D. RISS Database Information Collection

1. Data submitted to RISSIntel, the RISSGang intelligence database, RISSafe, RISS7 instances, or any other RISS-maintained database is owned by originating agencies.
2. RISS and participating agencies using the RISS databases shall comply with and adhere to all laws and regulations, including, but not limited to:
   a. 28 CFR Part 23 regarding collection of criminal intelligence information.
   b. The Organisation for Economic Co-operation and Development's Fair Information Principles (FIPs) (http://it.ojp.gov/documents/OECD_FIPs.pdf), which include:

      - Collection Limitation Principle
      - Data Quality Principle
      - Purpose Specification Principle
      - Use Limitation Principle
      - Security Safeguards Principle
      - Openness Principle
      - Individual Participation Principle
      - Accountability Principle

   c. NCISP recommendations regarding information and intelligence sharing.
   d. Applicable constitutional, statutory, regulatory, and administrative rules and other legal provisions, as well as any other DOJ regulations that apply to multijurisdictional criminal intelligence databases.
3. External agencies that access and share information with the RISS Program shall comply with the laws and regulations governing those individual agencies in addition to this privacy policy, other RISS policies, and applicable laws and regulations.
4. RISS will partner only with entities that provide appropriate assurances that their methods for gathering personally identifiable information comply with applicable laws and regulations and that these methods are based on lawful information collection practices.

5. RISS will not seek or retain information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or event; or their race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation.
6. To the maximum extent possible, information received from RISS by originating agencies will be labeled (by record, data set, or system of records), pursuant to applicable limitations on access and sensitivity of disclosure to:
    a. Protect confidential sources and police undercover techniques and methods.
    b. Not interfere with or compromise pending criminal investigations.
    c. Protect an individual's right of privacy and his or her civil rights and civil liberties.
    d. Provide legally required protections based on the individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.

E. Data Quality

1. RISS will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources; accurate, current, and complete, including the relevant context in which it was sought or received and other related information; and properly merged with other information about the same individual or organization. (See Section 4. G. below pertaining to merging/linking of records information.)
2. Originating agencies external to RISS are responsible for the quality and accuracy of the data accessed by or provided to RISS. If data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable, RISS will advise the appropriate contact person, in writing or electronically, in the originating agency. The originating agency is responsible for then confirming (as accurate), correcting, or purging the information from the RISS resource within a reasonable time. Recipients of the information will be notified of errors or deficiencies that may affect the rights of the subject of the information.
3. Depending upon the resource (e.g., RISSIntel, RISSGang, RISSafe), data provided by authorized users to RISS-supported systems shall:
    a. Be based on proper criminal predicate or threat to public safety;
    b. Be based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal or terrorist activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal (including terrorist) conduct or activity;
    c. Be relevant to the investigation and prosecution of suspected criminal or terrorist incidents; the enforcement of sanctions, orders, or sentences; or the prevention of crime;
    d. Be relevant in a criminal analysis or in the administration of criminal justice and public safety (including topical searches);
    e. Support authorized public safety and private sector efforts, as appropriate, and facilitate information sharing and communications among these entities; or
    f. Protect officer safety and ensure the integrity of investigative efforts.

    The data shall also be derived from a source that is reliable and information that has been verified or where limitations on the information's quality are identified. The information

must be collected in a lawful manner, with the knowledge and consent of the individual, if appropriate.

F. Collation and Analysis

1. Users submitting information to RISS-supported systems are authorized individuals from member agencies or appropriate nonmember law enforcement, public safety, or private sector entities. These individuals are sworn law enforcement officers, intelligence analysts, criminal justice officials, public safety officials, and appropriate critical infrastructure and private entity officials.
2. As necessary, RISS may provide limited information, such as contact phone numbers, to appropriate RISS members to facilitate communications and enhance information sharing. For example, ATIX Participant information is provided at the secure ATIX website for participants to obtain phone numbers of individuals addressing similar public safety issues. (See Section 6 for additional information.)
3. Users are permitted to access only information and systems specifically authorized for their use.
4. Information acquired or received by RISS or accessed from other sources will be analyzed only by qualified individuals who have successfully completed a background check and appropriate security clearance, if applicable, and who have been selected, approved, and trained accordingly.
5. RISS may acquire or receive the following types of information: criminal intelligence, criminal history, investigative case information, SBU information, other investigative data (such as information housed in the RISS Pawnshop Database, the Pseudo Violator Tracking System, and the Cold Hit Outcome Project), terrorism-related suspicious activity reports, and public record information.
6. Information acquired or received by RISS or accessed from other sources is analyzed according to priorities and needs to:
   a. Further crime prevention (including terrorism), law enforcement, force deployment, or prosecution objectives and other priorities established by RISS;
   b. Provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal or terrorist activities;
   c. Support investigations, including those of gang activity, criminal violence, illegal narcotics, cybercrime, terrorism, human trafficking, identity theft, and other appropriate crimes;
   d. Support and facilitate public safety and private sector efforts safeguarding critical infrastructure and responding to disasters; or
   e. Ensure officer safety.

G. Merging/Linking of Records

1. Records regarding an individual or organization from two or more sources will not be merged by RISS Center staff.
2. Records may be linked by authorized RISS personnel when there is sufficient identifying information to reasonably conclude that the information is about the same individual or

organization. In order to link information, authorized RISS personnel shall review all available attributes and ascertain a set of identifiers that support a high degree of accuracy.

H. Access

1. Credentialed, role-based access criteria will be used by RISS, as appropriate, to control:
   a. The information to which a particular group or class of users can have access based on the group or class.
   b. The information a class of users can add, change, delete, or print.
   c. To whom, individually, the information can be disclosed and under what circumstances.
2. RISS employs and continuously reviews and refines appropriate security and privacy control measures—including physical, electronic, and organizational measures—to ensure that individual identification information is safeguarded and is not compromised.
3. All individuals having access to RISS resources agree to the following:
   a. Criminal intelligence and law enforcement databases accessible via RISSNET will be used only to perform official law enforcement investigative-related duties in a manner authorized by the user's employer.
   b. Individual passwords will not be disclosed to any other person.
   c. Individual passwords will be changed if authorized personnel of the agency suspect the password has been improperly disclosed or otherwise compromised.
   d. Use of RISS in an unauthorized or illegal manner will subject the user to denial of further use of RISS resources, discipline by the user's employing agency, and/or criminal prosecution. Each authorized user understands that access to RISS can be denied or rescinded for failure to comply with the applicable restrictions and use limitations.
4. Users are permitted to access only information and systems specifically authorized for their use.
5. Users must complete an Individual User Agreement or equivalent application or acknowledgement or be covered by an interagency Memorandum of Understanding (MOU), in conjunction with training provided.
6. RISS retains the right to suspend or withdraw membership and user privileges, as deemed appropriate, in instances of violation of this or any other RISS policy.
7. All users are subject to the RISS Privacy Policy, the RISSNET Security Policy, the RISSNET Electronic Communications Policy, the RISSNET Remote User Authentication and Access Control Policy, and other RISS-related policies.
8. Use of RISSNET is limited to those individuals who have successfully completed the RISS identification and approval process or who are part of an interagency MOU and have received appropriate training (users).
9. In order to confirm the identity of individual RISSNET users and to ensure that user impersonation is prevented, RISSNET users must provide a variety of personal information about themselves to enable RISS to ensure that only appropriate individuals are permitted access to information for which they have a "need to know" and "right to know." Personally identifiable information provided by authorized users for this purpose, including membership and user information, shall be protected under this policy. (See Section 6 for additional information.)

I. Security

1. RISS will operate secure facilities, whereby personnel maintain appropriate identification to enter the facility and visitors are required to check in and sign in upon entry. The facilities must also meet all appropriate local and state laws and ordinances.
2. RISS will ensure that security procedures are in place in order to safeguard human life and property.
3. RISS will employ secure internal and external safeguards against network intrusion.
4. Access to RISSNET resources will be allowed using only secure networking technologies, such as RISSNET's IPsec VPN or RISSNET's Multiprotocol Label Switching (MPLS) circuits.
5. RISS will grant access to its resources only to RISS staff or appropriate personnel whose positions and job duties require such access.
6. RISS will store information in a manner that ensures it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions.
7. Queries made to RISS's data applications will be logged into the data system identifying the user initiating the query.
8. RISS will utilize watch logs to maintain audit trails of requested and disseminated information.
9. To prevent public records disclosure, risk and vulnerability assessments will not be stored with publicly available data.
10. If information is believed to have been breached or obtained by an unauthorized person and access to such information threatens physical, reputational, or financial harm to another person, RISS will notify the originating agency of the breach. The originating agency will notify the individual about whom personal information was breached or obtained. The notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or any measures necessary to determine the scope of the release of information and, if necessary, to reasonably restore the integrity of any information system affected by this release. The originating agency will notify RISS that notification was made.

J. Use

1. Use of RISS resources is limited to those individuals who have successfully completed the RISS identification and approval process or who are part of an interagency MOU and have received appropriate training (users).
2. Information obtained through RISS can be used only for the lawful performance of duties and/or for the purposes necessary for effective administration of RISSNET and RISSNET resource authentication and access control procedures.
3. Information obtained through or stored by RISS cannot be (1) sold, published, exchanged, or disclosed for commercial purposes; (2) disclosed or published without prior approval of the contributing agency; or (3) disseminated to unauthorized persons.

K. Training

1. **RISS Staff**—RISS will ensure that appropriate staff is trained on this privacy policy.
   a. Training will address the substance of the policy and its importance to RISS's mission and staff members' responsibility, including potential consequences of violating the policy.
   b. The level and amount of training for RISS staff will be based on a staff member's position and access/use of investigative and intelligence data. At a minimum, RISS staff members will complete the 28 CFR Part 23 Online Training course, review and acknowledge the RISS Privacy Policy, and agree to comply with the tenets of this policy.
   c. Additional training will be provided for staff members with direct contact with investigative or intelligence data.
2. **Partners/Contractors/Others**—RISS and the partnering entity will discuss appropriate provisions of this policy during the initial planning and negotiations phase. Member agencies, users, contractors, and other partners are expected to review the tenets of their agreements with RISS, which will include appropriate language from this policy and refer to the full policy and its location.
3. A copy of the RISS Privacy Policy will be made available upon request. The latest version of this policy will be posted at the RISS public website, www.riss.net.

Section 5: Other Investigative Databases and Sources

Each RISS Center employs personnel with expertise in intelligence research, analytical services, law enforcement, criminal justice, and information technology. In order to meet the mission of the RISS Program, RISS Center staff, on behalf of member law enforcement officers, access, utilize, search, analyze, and compile information from a variety of data sources, including those developed and operated by RISS—as well as other data sources—such as commercial databases, motor vehicle records, investigative databases, deconfliction, criminal history information, and suspicious activity reporting (SAR) information.

Investigative data sources that are not owned and operated by RISS may be used by authorized RISS Center staff to assist member law enforcement officers in identifying investigative leads; locating suspects, witnesses, victims, addresses, phone numbers, and other critical elements of a target; developing analytical products; and to assist in furthering an investigation. RISS does not gather, collect, or seek information to populate these resources. Access to these resources is based on a "need-to-know" and "right-to-know" basis. Authorized RISS Center staff are permitted to only query these sources and view records; they may not edit data in these sources. However, RISS staff may conduct analyses and develop intelligence briefings or materials, as requested by an officer. If terrorism-related SAR data is included in that package, the information must comply with the collection, retention, and purge policies pertaining to such data and contained in this policy.

A. Investigative and Commercial Databases

1. Each RISS Center has obtained access to a variety of investigative and commercial databases used to obtain subscription and other investigative information.

2. RISS will partner only with entities that provide appropriate assurances that their methods for gathering personally identifiable information comply with applicable local, state, territorial, federal, and tribal laws and regulations and that these methods are based on lawful information collection practices.
3. RISS will make every reasonable effort to ensure that information obtained from these resources is derived from dependable and trustworthy sources; accurate, current, and complete, including the relevant context in which it was sought or received and other related information; and properly merged with other information about the same individual or organization. (See Section 4. G. pertaining to merging/linking of records for more information.)
4. Originating agencies external to RISS are responsible for the quality and accuracy of the data accessed by or provided to RISS. If data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable, RISS will advise the appropriate contact person, in writing or electronically, in the originating agency.

B. Suspicious Activity Information

1. As part of the Nationwide Suspicious Activity Reporting Initiative (NSI), RISS Center staff may be granted access to terrorism-related suspicious activity reporting information (also known as an Information Sharing Environment Suspicious Activity Report—ISE-SAR) contained in the NSI ISE-SAR shared space.
2. Authorized RISS Center staff shall be granted VIEW-only rights and will not be authorized to download, populate, or edit data.
3. Only RISS Center staff who have successfully completed NSI-approved analyst/investigator training shall be provided access to the NSI ISE-SAR shared space.
4. At the request of a member agency officer, RISS Center staff may query the NSI ISE-SAR shared space. Results will be provided back to the requesting officer, along with any other appropriate results from other sources.
5. RISS will store and provide access to ISE-SAR information using the same method used for data which rises to the level of reasonable suspicion and which includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information.
6. RISS will utilize this information for law enforcement purposes only and comply with all aspects of this policy in the use and dissemination of such data.

Section 6: Agency and User Information

Officers, analysts, and other appropriate users provide personal identifiers in order to receive access to RISSNET-related resources. Information includes, but is not limited to, the following:

1. Name
2. Title/Rank/Position
3. Organization/Agency/Department, Address, Phone Number, and Fax Number
4. Date of Birth/Place of Birth
5. Cell Phone
6. E-Mail Address(es)

7. Personal Challenge Questions (facts about a user that are not common knowledge and not likely to change)

This information is gathered in order to provide access to RISS's automated resources, as well as other services and programs. RISS maintains this information in a secure environment and utilizes this information only in its mission to provide support and services to law enforcement and other criminal justice entities, to further information sharing, to ensure compliance with this policy and other appropriate laws and regulations, and for auditing purposes.

RISS shall not sell, publish, exchange, or disclose user information without prior approval of the officer, analyst, or appropriate individual.

RISS Center staff will regularly review membership and participant information to ensure accuracy. RISS will make every effort to ensure that the information is accurate and complete. RISS will request updates from agencies and update/delete records as agency contacts change, officers/analysts leave employment, etc.

Agency and user information is also subject to Section 4 of this policy.

Section 7: Audits

A. Section 4 of this privacy policy addresses RISS criminal intelligence databases regarding compliance with 28 CFR Part 23. RISS shall abide by the auditing requirements within that guideline.
B. Systems that are not required to be 28 CFR Part 23-compliant, such as investigative databases, will maintain an appropriate electronic log or auditing capability where available.
C. RISS will store information in a manner that ensures it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions.
D. Queries made to RISS's data applications will be logged into the data system identifying the user initiating the query.
E. RISS will utilize watch logs to maintain audit trails of requested and disseminated information. RISS will routinely monitor logs for indications of unusual activity and take appropriate action, if necessary.
F. To prevent public records disclosure, risk and vulnerability assessments will not be stored with publicly available data.

Section 8: Evaluation and Monitoring

A. RISS will continuously evaluate and monitor its resources, technologies, security practices, and associated processes to ensure compliance with this and all appropriate RISS policies.
B. RISS will, through its six RISS Centers, conduct 28 CFR Part 23 compliance reviews of member agency processes. DOJ or RISS may request a third party to conduct additional reviews, as needed and appropriate.
C. RISS will ensure that only appropriate personnel have access to staff, member, and user information.

D. RISS will revise its practices, as appropriate, to ensure continued compliance and to stay abreast of issues impacting the privacy policy arena in order to ensure that all RISS policies and practices are up to date and appropriate.
E. RISS will adopt and follow procedures and practices to ensure and evaluate the compliance of users in abiding by the provisions in this policy and with applicable law. This will include regular audits of the information and intelligence.
F. Requests or questions regarding this policy may be directed to the individual RISS Director covering the appropriate region. A list of the RISS Directors and their contact information is provided at www.riss.net.

Section 9: Accountability

A. RISS Center staff or authorized users shall report violations or suspected violations of this policy to their immediate supervisor, as well as to the in-region RISS Center. The in-region RISS Center Director may resolve the matter as appropriate, engage assistance and consultation from the other Directors, and/or seek legal support to resolve the issue. Items arising that may impact all of the centers or the RISS Program's national initiatives shall be discussed and deliberated by the RNPG for resolution.
B. If an authorized user is found to be in violation of the provisions of this policy, the RISS Center reserves the right to suspend or discontinue access to information by the user and/or request that the relevant member or nonmember agency, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions.
C. If any RISS Center staff member is found to be in violation of any provision of this policy, the RISS Center will reprimand, suspend, demote, transfer, or terminate the individual, as authorized by applicable personnel policies.
D. In case of user or staff violations of the law, the RISS Center will refer the matter to appropriate authorities for criminal prosecution, as necessary, to comply with the law and effectuate the purposes of this policy.

Section 10: Revision and Amendments

A. The RNPG has the authority to amend any part(s) of this policy, as appropriate.
B. At least annually, the RNPG will review this policy for content, relevancy, and effectiveness and update the provisions protecting privacy, civil rights, and civil liberties contained in this policy, making appropriate changes in response to implementation experience, changes in applicable law and technology, the purpose and use of the information systems, and public expectations.
C. A representative from a RISS Center, a RISS Director, the RISS Chief Information Officer (CIO), the RTSC Manager, or other appropriate entity may request a change or revision to this policy by contacting the chair of the RNPG and will provide details regarding the proposed change and the reason/justification for the change. The requestor will provide feedback/discussion on the issue. Once any change is approved by the RNPG, the change will be made to this policy and a new version of this policy will be distributed. The staff, users, members, and other participants and partners will adhere to the most recent version of this privacy policy.
D. If changes occur to related policies, laws, or regulations, such as other RISS policies or 28 CFR Part 23, the RNPG may revise this policy, as appropriate.
E. Approved amendments to this policy shall be documented in appropriate RISS meeting minutes, and the date of such action shall be logged herein.