Rhode Island State Fusion Center
Rhode Island State Police
311 Danielson Pike
North Scituate, RI 02857

PRIVACY POLICY

I. Mission Statement

The Mission of the Rhode Island State Fusion Center is to facilitate the efficient, timely and accurate exchange of information between local, state and federal public safety agencies and private sector organizations. Through a cooperative and coordinated approach, the Fusion Center will augment law enforcement operations by acting as a centralized, comprehensive criminal intelligence center to coordinate the exchange of criminal information on a statewide basis. The Fusion Center will collect, analyze and disseminate intelligence information in an effort to identify, investigate and prevent criminal activity relevant to terrorism and public safety.

II. Purpose

The Rhode Island State Fusion Center ("RIFC") was established in March of 2005. The Center is staffed by eight (8) full-time personnel representing the Rhode Island State Police ("RISP"), Department of Homeland Security ("DHS"), and Providence Police Department ("PPD"). The personnel consist of Intelligence Analysts, Police Officers, Special Agents and Program Managers. The RIFC is co-located with the Providence Office of the Federal Bureau of Investigation ("FBI"), specifically the Joint Terrorism Task Force ("JTTF"). This co-location allows for the proactive exchange of information and for collaboration between the various agencies.

A. The purpose of this privacy policy is to ensure safeguards and sanctions are in place to protect personal information as information and intelligence are developed, exchanged and assists its authorized users in:

1. Increasing public safety and improve national security.
2. Minimizing the threat and risk of injury to specific individuals.
3. Minimizing the threat and risk of injury to law enforcement and others responsible for public protection, safety, or health.
4. Preventing and disrupt potential terrorist attacks.
5. Protecting individual privacy, civil rights, civil liberties, and other protected interests.
6. Minimizing the threat and risk of damage to real or personal property.

7. Protecting the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information.
8. Minimizing reluctance of individuals or groups to use or cooperate with the justice system.
9. Supporting the role of the justice system in society.
10. Promoting governmental legitimacy and accountability.
11. Not unduly burden the ongoing business of the justice system.
12. Make the most effective use of public resources allocated to justice agencies.

III. Compliance with Laws regarding Privacy, Civil Rights and Civil Liberties:

A. All RIFC personnel, participating agency personnel, personnel providing information technology services to the center, private contractors, and other authorized users will comply with the center's privacy policy. This policy applies to information the center gathers or collects, receives, maintains, stores, accesses, discloses, or disseminates to center personnel, governmental agencies (including Information Sharing Environment [ISE] participating centers and agencies), and participating justice and public safety agencies, as well as to private contractors, private entities, and the general public.

1. All RIFC personnel, participating agency personnel, personnel providing information technology services to the center, private contractors, agencies from which center information originates, and other authorized users will comply with applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to the U.S. and Rhode Island constitutions and the General Laws of the State of Rhode Island, specifically The Civil Rights Act of 1990, RIGL 42-112 et seq. and the Right to Privacy law, RIGL 9-1-28.1

B. The RIFC has adopted internal operating policies requiring compliance with the General Laws of the State of Rhode Island, specifically The Civil Rights Act of 1990, RIGL 42-112 et seq. and the Right to Privacy law, RIGL 9-1-28.1, which protect privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing, and disclosure of information in the RIFC information system.

IV. Governance and Oversight:

A. The RIFC is overseen operationally by the RISP. A RISP Lieutenant runs the daily operational aspects of the RIFC. The RISP Lieutenant serves as the Privacy Officer for the Center and will be trained in Privacy and Civil Rights and Civil Liberty issues. The Privacy Officer is responsible for the direct oversight of the privacy policy, which ensures that privacy and civil rights are protected. The RIFC is guided by a designated privacy oversight committee to ensure that privacy and civil rights are protected as provided in this policy and by the center's information-gathering and collection, retention, and dissemination processes and procedures. The committee will annually

review and update the policy in response to changes in law and implementation experience, including the results of audits and inspections.

B. The Privacy Oversight Committee will be comprised of the RIFC director, RIFC deputy director, RISP legal advisor.

C. The RIFC's Privacy Officer ensures enforcement procedures and sanctions outlined in Section XIV.C. are adequate and enforced.

D. The Privacy Officer is the point of contact for reporting errors and violations of center's privacy policy. The Privacy Officer can be contacted at the following address: 311 Danielson Pike, North Scituate, Rhode Island 02857The RIFC is addressed in the RISP internal policies, where the overall mission and operation is defined. [See Appendix B, RISP General Order 77J, entitled, "Homeland Security-Fusion Center."]

V. Definitions

A. Primary Terms and definitions used in the RIFC are located in Appendix A.

VI. Seeking and Retaining Information:

The RIFC serves as the hub for the receipt and dissemination of information related to all crimes and terrorism. The RIFC works with various federal, state, and local law enforcement agencies, as well as non-law enforcement groups such as the public health department, fire departments, campus police agencies, and the private sector.

A. What Information May Be Sought or Retained?

1. The RIFC will seek or retain only information:

a) Is based on a possible threat to public safety or the enforcement of the criminal law, or

b) Is based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or 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, or

c) Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime, or

d) Is useful in crime analysis or in the administration of criminal justice and public safety (including topical searches), and

e) The source of the information is reliable and verifiable or limitations on the quality of the information are identified, and

f) The information was collected in a fair and lawful manner, with the knowledge and consent of the individual, if appropriate.

g) The center may retain protected information that is based on a level of suspicion that is less than "reasonable suspicion," such as tips and leads or suspicious activity report (SAR) information, subject to the policies and procedures specified in this policy.

2. The RIFC will not seek or retain information about the political, religious, or social views; participation in a particular organization or event; or activities of any individual or his/her race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation unless such information is:

a) relevant to whether an individual or organization has engaged in, is engaging in, or is planning a criminal or terrorist activity;
b) an observable behavior or incident indicative of criminal activity or terrorist attack planning;
c) Needed by the RIFC to identify an individual in order to operate effectively, or to provide services to the individual, or accommodate an individual's religious, ethnic, or cultural requests or obligations.

3. The RIFC applies labels to agency-originated information (or ensures that the originating agency has applied labels) to indicate to the accessing authorized user that:

a) The information is protected information (See Appendix A, Definitions).
b) The information is subject to RIGL 38-2-1 Access to Public Records law restricting access, use, or disclosure.

4. The RIFC shall keep a record of the source of all information retained in compliance with 28 CFR Part 23 and applicable State of Rhode Island and RISP Records Retention Schedules. [See Appendix C, RISP General Order 2D entitled, "Records Retention Schedule."]

5. RIFC personnel are required to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention,

and security of tips and leads and suspicious activity report (SAR) information. Center personnel will:

a) Prior to allowing access to or dissemination of the information, ensure that attempts to validate or refute the information have taken place and that the information has been assessed for sensitivity and confidence by subjecting it to an evaluation or screening process to determine its credibility and value and categorize the information as unsubstantiated or uncorroborated if attempts to validate or determine the reliability of the information have been unsuccessful. The center will use a standard reporting format and data collection codes for SAR information.

b) Store the information using the same storage 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.

c) Allow access to or disseminate the information using the same (or a more restrictive) access or dissemination standard that is used for data that rises to the level of reasonable suspicion (for example, "need-to-know" and "right-to-know" access or dissemination for personally identifiable information).

d) Regularly provide access to or disseminate the information in response to an interagency inquiry for law enforcement, homeland security, or public safety and analytical purposes or provide an assessment of the information to any agency, entity, individual, or the public when credible information indicates potential imminent danger to life or property.

e) Retain information for one year in order to work an unvalidated tip, lead, or SAR information to determine its credibility and value or assign a "disposition" label (for example, undetermined or unresolved, cleared or unfounded, verified, or under active investigation) so that a subsequently authorized user knows the status and purpose for the retention and will retain the information based on the retention period associated with the disposition label.

f) Adhere to and follow the center's physical, administrative, and technical security measures to ensure the protection and security of tips, leads, and SAR information. Tips, leads, and SAR information will be secured in a system that is the same as or similar to the system that secures data that rises to the level of reasonable suspicion.

6. The RIFC incorporates the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious activities and incidents (SAR process) into existing processes and systems used to manage other crime-related information and criminal intelligence, thus leveraging existing policies and protocols utilized to protect the information, as well as information privacy, civil rights, and civil liberties.

7. The RIFC will identify and review protected information that may be accessed from or disseminated by the center prior to sharing that information through the Information Sharing Environment. Further, the center will provide notice mechanisms, including but not limited to metadata or data field labels, that will enable ISE authorized users to determine the nature of the protected information and how to handle the information in accordance with applicable legal requirements.

B. Methods of Seeking or Receiving Information.

1. Information gathering and investigative techniques used by the RIFC and originating agencies will comply with all applicable law and guidance, including:

a) 28 CFR Part 23 for criminal intelligence information

b) Organization for Economic Co-operation and Development *Fair Information Practices* (under certain circumstances, there may be exceptions to the Fair Information Principles, based, for example, on authorities paralleling those provided in the federal Privacy Act; state, local, and tribal law; or center policy).

c) Applicable criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) *National Criminal Intelligence Sharing Plan* (NCISP).

2. The RIFC's SAR process provides for human review and vetting to ensure that information is both legally gathered and, where applicable, determined to have a potential terrorism nexus. Law enforcement officers and appropriate center and participating agency staff will be trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism.

3. The RIFC's SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved in activities that have been determined to be consistent with criminal activities associated with terrorism will be documented and shared through the ISE. These safeguards are intended to ensure that information that could violate civil rights (race, religion, national origin, ethnicity, etc.) and civil liberties (speech, assembly, religious exercise, etc.) will not be intentionally or inadvertently gathered, documented, processed, and shared.

4. The RIFC will not directly or indirectly receive, seek, accept, or retain information from an individual or non-government information provider, who may or may not receive a fee or benefit for providing the information, if the agency knows or has reason to believe that:

   a) the individual or information provider is legally prohibited from obtaining the specific information sought or disclosing it to the agency;
   b) the individual or information provider used methods for collecting the information that the agency itself could not legally use;
   c) the specific information sought from the individual or information provider could not legally be collected by the RIFC; or,
   d) the RIFC has not taken the steps necessary to be authorized to collect the information.

5. Information gathering and investigative techniques used by the RIFC will be no more intrusive or broad scale than is necessary in the particular circumstance to gather information it is authorized to seek or retain pursuant to Section VII.A.

6. External agencies that receive and share information with the RIFC are governed by laws and rules governing those agencies as well as by applicable federal and state laws.

7. The RIFC will contract only with commercial database entities that provide an assurance their methods for gathering personal identifiable information (PII) comply with applicable authorities and these methods are not based on misleading information collection practices.

VII. Classification of Information

A. Regarding Validity and Reliability.

1. At the time of retention in the system, the information will be labeled regarding its content validity, nature of the source, and source reliability.

   a) Whether the information is based upon a standard of reasonable suspicion of criminal activity;

   b) Whether the information consists of tips and leads data or suspicious activity reports;

   c) The nature of the source as it affects veracity (for example, anonymous tips, trained interviewer or investigator, public record, private sector); and

   d) The validity of the content (for example, verified partially verified, unverified, or unable to verify

   e) The reliability of the source (for example, reliable, usually reliable, unreliable, unknown).

B. The labeling of retained information will be reevaluated by the RIFC or the originating agency when new information is gathered that has an impact on confidence (source reliability and content validity) in previously retained information.

C. **Regarding Limitations on Access and Disclosure.**

1. At the time a decision is made by the RIFC to retain information, it will be labeled (by record, data set, or system of records), to the maximum extent feasible, pursuant to applicable limitations on access and sensitivity of disclosure to:

   a) Protect confidential sources and law enforcement undercover techniques and methods.
   b) Not interfere with or compromise pending criminal investigations.
   c) Protect an individual's right of privacy or 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.

2. The classification of existing information will be reevaluated whenever new information is added that has an impact on access limitations or the

sensitivity of disclosure of the information; or there is a change in the use of the information affecting access or disclosure limitations.

3. Access to RIFC information:

   a) The RIFC Director, and/or administrator(s) designated by the Director, shall establish requirements and record all personnel as to their access authority and permission to access RIFC's information;

   b) Permissions regarding viewing, adding, and printing of RIFC information is controlled by RIFC's administrator (s);

   c) All RIFC personnel, with approval from the Director, or his designee, may disclose RIFC information pursuant to applicable policy;

   d) An audit trail shall be maintained regarding access to, and disclosure of, RIFC information

4. The access classifications will be used to control what information a class of users can have access to; what information a class of users can add, change, delete, or print; and to whom the information can be disclosed and under what circumstances.

VIII. Information Quality.

A. RIFC will make every reasonable effort to ensure that information sought or retained is:

1. derived from dependable and trustworthy sources of information;
2. accurate;
3. current;
4. complete, including the relevant context in which it was sought or received and other related information; and,
5. merged with other information about the same individual or organization only when the applicable standard in Section VII.A. has been met.
6. At the time of retention in the system, the information will be labeled regarding its level of quality (accuracy, completeness, currency, and confidence [verifiability and reliability])

B. RIFC will make every reasonable effort to ensure that only authorized users are allowed to add, change, or delete information in the system.

C. The RIFC will conduct periodic data quality reviews of information it originates and make every reasonable effort to ensure that the information will be corrected, deleted from the system, or not used when the center identifies information that is erroneous,

misleading, obsolete, or otherwise unreliable; the center did not have authority to gather the information or to provide the information to another agency; or the center used prohibited means to gather the information (except when the center's information source did not act as the agent of the center in gathering the information).

D. Originating agencies external to the RIFC are responsible for reviewing the quality and accuracy of the data provided to the center. The center will review the quality of information it has received from an originating agency and advise the appropriate contact person in the originating agency, in writing or electronically and telephonically if necessary, if its data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable.

E. The RIFC investigates, in a timely manner, alleged errors and deficiencies (or refers them to the originating agency) and corrects, deletes, or refrains from using protected information found to be erroneous or deficient.

F. The RIFC will use electronic and telephonic, (if necessary) notification to inform recipient agencies when information previously provided to the recipient agency is deleted or changed by the center because the information is determined to be erroneous, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the rights of the individual may be affected.

G. The RIFC will attach (or ensure that the originating agency has attached) specific labels and descriptive metadata to information that will be used, accessed, or disseminated to clearly indicate any legal restrictions on information sharing based on information sensitivity or classification.

H. The RIFC requires certain basic descriptive information labels to be entered and electronically associated with data for which there are special laws, rules, or policies regarding access, use, and disclosure, including terrorism-related information shared through the ISE. The types of information include:

1. The name of the originating center, department or agency, component, and subcomponent.
2. The name of the center's justice information system from which the information is disseminated.
3. The date the information was collected and, where feasible, the date its accuracy was last verified.
4. The title and contact information for the person to whom questions regarding the information should be directed.

IX. Collation and Analysis of Information.

A. Information sought or received by RIFC or from other sources will only be analyzed:

1. by qualified individuals who have successfully passed a background check and have been properly trained;
2. to 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, including terrorist, activities generally; and,
3. to further crime and terrorism prevention, enforcement, force deployment, or prosecution objectives and priorities established by the agency.

B. Information sought or received by the RIFC or from other sources will not be analyzed or combined in a manner or for a purpose that violates Section IX.

C. Information subject to collation and analysis is information as defined and indentified in Section VI.

X. Merging of Information from Different Sources.

A. Information about an individual or organization from two or more sources will not be merged unless there is sufficient identifying information to reasonably conclude that the information is about the same individual or organization.

B. The set of identifying information sufficient to allow merging will utilize reasonable steps to identify the subject, and may include the name (full or partial) and, in most cases, one or more of the following: date of birth; law enforcement or corrections system identification number individual identifiers such as fingerprints, photographs, physical description, height, weight, eye and hair color, race, ethnicity, tattoos, marks or scars; social security number; driver's license number; other biometrics such as DNA, retinal scan, or facial recognition. Identifiers or characteristics that, when combine, could clearly establish that the information from multiple records is about the same organization may include the organization's name, federal or state tax ID number, office address, and telephone number.

C. If the matching requirements are not fully met but there is a strong partial match, the information may be associated if accompanied by a clear statement that is has not been adequately established that the information relates to the same individual or organization.

XI. Sharing and Disclosure of Information.

A. Sharing Information within the RIFC and with other Justice System Partners.

1. Access to information retained by the RIFC will only be provided to persons within the RIFC or in other governmental agencies who are authorized to have access and only for legitimate law enforcement, public protection, public prosecution, public health, or justice purposes and only for the performance of official duties in accordance with the law and procedures applicable to the agency for whom the person is working.

2. The RIFC adheres to the current version of the ISE-SAR Functional Standard for its suspicious activity reporting (SAR) process, including the use of a standard reporting format and commonly accepted data collection codes and a sharing process that complies with the ISE-SAR Functional Standard for suspicious activity potentially related to terrorism.

3. Agencies external to the RIFC may not disseminate RIFC information received from RIFC without prior approval from the originator of the information.

4. An audit trail will be kept of access by or dissemination of information to such persons.

B. Sharing Information with those Responsible for Public Protection, Safety, or Public Health.

1. Information retained by the RIFC may be disseminated to individuals in public or private entities only for public protection, safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures.

2. Nothing in this policy shall limit the dissemination, including unsolicited, of an assessment of criminal intelligence information to a government official or to any other individual, when necessary to avoid imminent danger or certain danger to life or property.

3. The agency shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.

4. An audit trail will be kept of the access by or dissemination of information to such persons.

C. Sharing Information for Specific Purposes.

1. Information gathered and retained by the RIFC may be disseminated for specific purposes upon request by persons authorized by law to have such access and only for those uses or purposes specified in the law.

   a) Government officials, public agencies, licensing boards, and certain nongovernmental agencies may be entitled to information about the criminal history of an individual applying for services, employment or benefits, if defined in Rhode Island General Laws.

   b) Disclosure of said information will be in compliance with the RISP RILETS policy. [See Appendix D, RISP General Order 54J entitled, "Rhode Island Law Enforcement Telecommunications System Policy and Procedures."]

2. The RIFC shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.

3. The audit trail will be kept of the requests for access and of what information is disseminated to such persons.

XII. Disclosure of information.

A. To the Public.

1. Information gathered and retained by the RIFC may be disclosed to a member of the public only if the information is defined by law to be a public record and is not accepted from disclosure by law, and it may only be disclosed in accordance with the law and procedures applicable to RIFC for this type of information.

2. The agency shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself, unless otherwise required by law.

3. An audit trail will be kept of all requests and of what information is disclosed to a member of the public.

4. The RIFC is authorized and shall charge a fee pursuant to RIGL § 38-2 **et seq**. – Access to Public Records Act.

B. To the Individual about Whom Information has been gathered.

1. Upon satisfactory verification of his/her identity and subject to the conditions specified in (b), an individual is entitled to know the existence of and to review the information about him/herself that has been gathered and retained by the RIFC. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information. The RIFC's response to the request for information will be made within a reasonable time and in a form that is readily intelligible to the individual.

2. The existence, content, and source of the information will not be made available to an individual when it is exempt from disclosure by law, including, but not limited to, RIGL 38.2, Access to Public Records, other Rhode Island law, or Federal law, including when:

   a) disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution (RIGL 38-2-2(4)(D)(a);

   b) disclosure would endanger the physical safety of any individual RIGL 38-2-2(4)(D)(f);

   c) the information is in a criminal intelligence system subject to 28 CFR Part 23 or is otherwise required to be kept confidential by

federal law or regulation or state law or rule of court (RIGL 38-2-4(S);

d) the information would reveal scientific and technological secrets or the security plans of military and law enforcement agencies, the disclosure of which would endanger the public welfare and security (RIGL 38-2-2(4)(F);

e) Information that meets the definition of "classified information" as that term is defined in the National Security Act, Public Law 235, Section 606 and in accord with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010; or

f) Disclosure would constitute an unwarranted invasion of personal privacy (RIGL 38-2-2(4)(D)(c))

3. Information gathered or collected and records retained by the RIFC will not be:

a) Sold, published, exchanged, or disclosed for commercial purposes; RIGL 38-2-6 Access to Public records

b) Disclosed or published without prior notice to the originating agency that such information is subject to disclosure or publication, unless disclosure is agreed to as part of the normal operations of the agency.

c) Disseminated to persons not authorized to access or use the information.

4. The RIFC may charge a reasonable fee that reflects the cost to the RIFC for search and retrieval of documents, and providing copies. These fees shall not exceed those set forth in RIGL 33-2-4 – Access to Public Records Act: Cost.

5. A record will be kept by the RIFC of all requests and of what information is disclosed to an individual.

6. There are several categories of records that will ordinarily not be provided to the public:

a) Records required to be kept confidential by law are exempted from disclosure requirements under the Access to Public Records Act, RIGL 38-2-4(S).

b) Information that meets the definition of "classified information" as that term is defined in the National Security Act, Public Law 235, Section 606.

c) Investigatory records of law enforcement agencies that are exempted from disclosure requirements under. However, certain

law enforcement records must be made available for inspection and copying under the Access to Public Records Act, RIGL 38-2-2(4)(D)(a)-(f).

d) A record or part of a record the public disclosure of which would have a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack is exempted from disclosure. This includes a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism or an act of agricultural terrorism, including vulnerability assessments, risk planning documents, needs assessments, and threat assessments under RIGL 38-2-2(4)(F); .

e) Protected federal, state, local, or tribal records, which may include records originated and controlled by another agency that cannot, under the Access to Public Records Act, RIGL 38-2-2(4)(S), be shared without permission.

C. Corrections and Appeals

1. If an individual has objections to the accuracy of completeness of the information retained about him/herself, the RIFC will inform the individual of the procedure for requesting review of any objections. The individual will be given reasons if a request for correction of information that has been disclosed to the individual is denied. The individual will also be informed of the procedure for appeal when the agency has declined to correct challenged information to the satisfaction of the individual about whom the information relates. A record will be kept of all requests for corrections and resulting action, if any.

D. Complaints

1. If an individual has a complaint with regard to the accuracy or completeness of terrorism-related protected information that:
    a) Is exempt from disclosure,
    b) has been or may be shared through the ISE, (b)
2. Is held by the RIFC and
    a) Allegedly has resulted in demonstrable
    b) harm to the complainant,

The center will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the center's Privacy Officer at the following address: 311 Danielson Pike, North Scituate, Rhode Island 02857. The Privacy Officer or will

acknowledge the complaint and state that it will be reviewed but will not confirm the existence or nonexistence of the information to the complainant unless otherwise required by law. If the information did not originate with the center, the Privacy Officer will notify the originating agency in writing or electronically within 10 days and, upon request, assist such agency to correct any identified data/record deficiencies, purge the information, or verify that the record is accurate. All information held by the center that is the subject of a complaint will be reviewed within 30 days and confirmed or corrected/purged if determined to be inaccurate or incomplete, to include incorrectly merged information, or to be out of date. If there is no resolution within 30 days, the center will not share the information until such time as the complaint has been resolved. A record will be kept by the center of all complaints and the resulting action taken in response to the complaint.

3. To delineate protected information shared through the ISE from other data, the RIFC maintains records of agencies sharing terrorism-related information and employs system mechanisms to identify the originating agency when the information is shared.

XIII. Information Retention and Destruction.

A. Review of Information Regarding Retention

1. Information will be reviewed for purging in accordance with 28 CFR Part 23, and outlined by GO-2D "RISP Records Retention Schedule" (The schedule consists of eighty (80) series of records recognized as those generated by the Division of State Police). Many of the retention periods are based on state and federal statute and regulation
2. When information has no further value or meets the criteria for removal under applicable law, it will be purged, destroyed, deleted, or returned to the submitting source.
3. A record of information to be reviewed for retention will be maintained by the RIFC, and for appropriate system(s), notice will be given to the submitter at least 30 days prior to the required review and validation/purge date.

B. Destruction of Information

1. The agency will delete information or return it to the source according to 28 CFR Part 23, and relevant RISP Records Retention Schedules.
2. Permission to destroy or return information or records will be obtained from RISP Legal Counsel for review, pursuant to RISP General Order 2D entitled, “Records Retention Schedule.”

3. Notification of proposed destruction or return of records will be provided to the RISP's Designated Records Custodian pursuant to RISP General Order 2D entitled, "Records Retention Schedule."

4. Notification of proposed destruction or return of records may or may not be provided to the originating agency by the RIFC, depending on the relevance of the information and any agreement with the originating agency.

5. A record that information has been purged or returned shall be maintained by the RIFC.

6. Notice will be given to the submitter at least 30 days prior to the required review and validation/purge date.

XIV. Accountability and Enforcement.

A. Information System Transparency.

1. A copy of the policy establishing protections of privacy, civil rights, and civil liberties will be made available to the public through an online request form on the Rhode Island State Police Web site (www.risp.ri.gov).

2. The RIFC has designated a person responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system and will provide to the public the Privacy Officer: 311 Danielson Pike, North Scituate, Rhode Island 0257.

3. The RIFC's Security Officer is designated and will be trained to serve as the center's Security Officer.

4. The RIFC will secure tips, leads, and SAR information in a separate repository system using security procedures and policies that are the same as or similar to those used for a system that secures data rising to the level of reasonable suspicion under 28 CFR Part 23.

5. Queries made to the RIFC's data applications will be logged into the data system identifying the user initiating the query.

6. RIFC will utilize watch logs to maintain audit trails of all types of information accessed, requested, and disseminated information. An audit trail will be kept for a minimum of on a monthly basis of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.

7. To prevent public records disclosure, risk and vulnerability assessments will not be stored with publicly available data.

8. The RIFC will follow the data breach notification guidance set forth in Office of Management and Budget Memorandum M-07-16 (May 2007, see http://www.whitehouse.gov/OMB/memoranda /fy2007/m07-16.pdf).

9. The main responsibility if the SSO will ensure information and the systems that contain information are secure.

B. Accountability for Activities

1. Primary responsibility for the operation of this justice information system, including operations; coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing, and disclosure of information; and the enforcement of this policy, is assigned to the RISP Lieutenant who is charged with overseeing the RIFC operations.
2. The RIFC will establish procedures, practices, and system protocols and use software, information technology tools, and physical security measures that protect information from unauthorized access, modification, theft, or sabotage, whether internal or external and whether due to natural or human-caused disasters or intrusions. The methods and techniques used shall be consistent with National Criminal Intelligence Sharing Plan, the RIFC Guidelines, Global's Applying Security Practices to Justice Information Sharing document, and 28 CFR Part 23.
3. The agency will store information in a manner such that it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions.
4. The RIFC will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of uses and the system itself with the provisions of this policy and applicable law. This will include logging access to these systems and periodic auditing of these systems, so as to not establish a pattern of the audits. These audits will be mandated at least annually and a record of the audits will be maintained by the Privacy Officer of the center.
5. The RIFC will require any individuals authorized to use the system to agree, in writing, to comply with the provisions of this policy and acknowledge receipt of this policy.
6. The RIFC will annually conduct audits and inspections of the information contained in the CrimeNtel system. The audits will be conducted randomly by a designated representative of the agency or by a designated independent party. The audit will be conducted in such a manner so as to protect the confidentiality, sensitivity, and privacy of the RIFC's information.
7. The RIFC shall annually review and will make appropriate changes to provisions protecting privacy, civil rights, and civil liberties in its policies and make appropriate changes in applicable law and public expectations.

8. The RIFC's personnel or other authorized users shall report errors and suspected or confirmed violations of center policies relating to protected information to the center's Privacy Officer.

9. The audit log of queries made to the RIFC will identify the user initiating the query.

C. Enforcement of Policy/NonCompliance

1. If center personnel, a participating agency or authorized user is suspected of or found to be not complying with the provisions of this policy regarding the collection, use, retention, destruction, sharing, classification, or disclosure of information, the RIFC will:

   a) suspend or discontinue access to information by the user;

   b) suspend, demote, transfer, or terminate the person(s) as permitted by applicable personnel policies;

   c) apply other sanctions or administrative actions as provided in agency personnel policies;

   d) request the agency, organization, contractor, or service provider employing the user to initiate proceedings to discipline the user or enforce the policy's provisions; or,

   e) refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

2. Disciplinary action, appropriate to the severity of the offense, should be taken against a user who:

   a) fails to comply with the provisions about the information may be sought or retained or what may not be sought or retained or who uses improper means or sources to seek or receive information;

   b) uses information for unauthorized purposes, including personal/commercial use, whether or not the person receives a benefit;

   c) discloses information to someone not authorized to receive the information;

   d) fail to correct information found to be erroneous or to report the error to appropriate personnel;

   e) fails to purge information when it is no longer of value or has reached its retention schedule;

   f) retains or otherwise fails to destroy information that is scheduled to be destroyed or is no longer relevant to the purposes of the system; or,

   g) fails to disclose information that an individual or the public is entitled, to know the existence of and to review.

3. The RIFC reserves the right to restrict the qualifications and number of personnel having access to center information and to suspend or withhold service and deny access to any participating agency or participating agency personnel violating the center's privacy policy.

XV. Training

A. The RIFC will require the following individuals to participate in training programs regarding the implementation of and adherence to the privacy, civil rights, and civil liberties polices.

1. Its personnel.
2. Personnel providing information technology services to the agency.
3. Staff in other public agencies or private contractors providingservices to the RIFC. Users who are not employed by the RIFC or acontractor.

B. The RIFC will provide special training regarding the center's requirements and policies for collection, use, and disclosure of protected information to personnel authorized to share protected information through the Information Sharing Environment

C. The training program will cover:

1. Purposes of the privacy, civil rights, and civil liberties protection policy.
2. Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the agency.
3. The impact of improper activities associated with information accessible within or through the agency.
4. Mechanisms for reporting violations of center privacy protection policies and procedures.
5. The nature and possible penalties for policy violations, including possible transfer, dismissal, civil and criminal liability, and immunity, if any.
6. Originating and participating agency responsibilities and obligations under applicable law and policy.
7. How to implement the policy in the day-to-day work of the user, whether a paper or systems user.

APPENDIX A
(Primary Terms & Definitions)

28 CFR Part 23 – Section 28 Part 23 of the Code of Federal Regulations. This code governs Criminal Intelligence Offices which receive federal funding to operate.

Access – Refers to the business rules, means, and processes by and through which agency participants obtain terrorism-related information, to include homeland security information, terrorism information, and law enforcement information acquired in the first instance by another agency participant.

Agency – Agency refers to the (name of agency) and all agencies that access, contribute, and share information in the (name of agency)'s justice information system.

Analysis – The function of handling, sorting, and filing information, including the sifting out of useless information, the orderly arrangement of collected materials so relationships can be established, and the creation of a system for rapid retrieval of filed information.

Assessment – An estimate, evaluation, or appraisal of information content and its possible impact.

Audit Trail – In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail—what commands were issued to the system, what records and files were accessed or modified, etc. Audit trails are a fundamental part of computer security, used to trace (albeit usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

Authorization – The process of granting a person, computer process, or device with access to certain information, services, or functionality. Authorization is derived from the identity of the person, computer process, or device requesting access that is verified through authentication.

Authorized User – A person that is granted direct access to RIFC information whose position and job duties require such access; who have successfully completed a background check and appropriate security clearance, if applicable; and who have been selected, approved, and trained accordingly.

Civil Rights – The term "civil rights" is used to imply that the state has a role in ensuring that all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of race, religion, gender, or other characteristics unrelated to the worth of the individual. Civil rights are, therefore, obligations imposed on government to promote equality. More specifically, they are the rights to personal liberty guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments, and by acts of Congress.

Civil Liberties – Civil liberties are fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights, the first ten Amendments to the Constitution of the United States. Civil liberties offer protection to

individuals from improper government action and arbitrary governmental interference. Generally, the term "civil rights" involves positive (or affirmative) government action, while the term "civil liberties" involves restrictions on government.

Classification – A rating given stored information. A classification indicates access and dissemination restrictions.

Collation – Assembling in proper order to clarify or give meaning to information

Confidentiality – Confidentiality is closely related to privacy, but is not identical. It refers to the obligations of individuals and institutions to use information under their control appropriately once it has been disclosed to them. One observes rules of confidentiality out of respect for, and to protect and preserve, the privacy of others. (See Privacy.)

Criminal Intelligence Information or Data – Information deemed relevant to the identification of, and the criminal activity engaged in, by an individual or organization that is reasonably suspected of involvement in criminal acts. The record is maintained in a criminal intelligence system per 28 CFR Part 23. Reasonable suspicion applies to the information.

Data – Insert symbols, signs, descriptions, or measures.

Data Breach—The unintentional release of secure information to an untrusted environment. This may include incidents such as theft or loss of digital media—including computer tapes, hard drives, or laptop computers containing such media—upon which such information is stored unencrypted; posting such information on the World Wide Web or on a computer otherwise accessible from the Internet without proper information security precautions; transfer of such information to a system that is not completely open but is not appropriately or formally accredited for security at the approved level, such as unencrypted e-mail; or transfer of such information to the information systems of a possibly hostile agency or environment where it may be exposed to more intensive decryption techniques

Data Protection – Data protection encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, use, protection, and disclosure of information.

Disclosure – The release, transfer, provision of access to, sharing, publication, or divulging of personal information in any manner – electronic, verbal, or in writing – to an individual, agency, or organization outside the agency that collected it. Disclosure is an aspect of privacy, focusing on information which may be available only to certain people for certain purposes but which is not available to everyone.

Dissemination – The transmission of intelligence orally, in writing, electronically, or by any other means, from the person having custody of the intelligence to another person.

Electronically Maintained - Information stored by a computer or on any electronic medium from which the information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, or compact disk optical media.

Electronically Transmitted - Information exchanged with a computer using electronic media, such as the movement of information from one location to another by magnetic or optical media, transmission over the Internet, intranet, extranet, leased lines, dial-up lines, private networks,

telephone voice response, and faxback systems. It does not include faxes, telephone calls, video teleconferencing, or messages left on voice mail

Information – Information includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists. Information received by law enforcement agencies can be categorized into four general areas: general data, tips and leads data, suspicious activity reports, and criminal intelligence information.

Information Collection - Information for submission to the RIFC can be collected from a variety of sources, including, but not limited to: informants, print and electronic media, public records, subpoenaed documents, and undercover operations. Collection will always be based upon reasonable suspicion of criminal activity, and will be conducted by lawful methods

Information Quality – Information quality refers to various aspects of the information; the accuracy and validity of the actual values of the data, data structure, and database/data repository design. Traditionally, the basic elements of information quality have been identified as accuracy, completeness, currency, reliability, and context/meaning. Today, information quality is being more fully described in multidimensional models, expanding conventional views of the topic to include considerations of accessibility, security, and privacy.

Information Sharing Environment (ISE) Suspicious Activity Report (SAR) (ISE-SAR)— A 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).

Intelligence – Information that has been processed (i.e., collected, evaluated, collated, analyzed, and reported). **Law –** As used by this policy, law includes any local, state, or federal statute, ordinance, regulation, executive order, policy, or court rule, decision, or order as construed by appropriate local, state, or federal officials or agencies.

Law Enforcement Information – Law enforcement information means any information obtained by, or of interest to, a law enforcement agency or official that is both (a) related to terrorism or the security of our homeland and (b) relevant to a law enforcement mission, including but not limited to information pertaining to an actual or potential criminal, civil, or administrative investigation, or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of, or response to, criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of or response to criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance.

Logs – Logs are a necessary part of an adequate security system because they are needed to ensure that data is properly tracked and that only authorized individuals are getting access to the data. ***(See also Audit Trail.)***

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 counter-terrorism activity, such as to further an investigation or meet another law enforcement requirement.

Originating Agency—The agency or organizational entity that documents information or data, including source agencies that document SAR (and, when authorized, ISE-SAR) information that is collected by a fusion center.

Personal Information – Information that can be used, either alone or in combination with other information, to identify individual subjects suspected of engaging in criminal activity, including terrorism.

Persons – Executive Order 12333 defines "United States persons" as United States citizens, aliens known by the intelligence agency concerned to be permanent resident aliens, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. For the intelligence community and for domestic law enforcement agencies, "persons" means United States citizens and lawful permanent residents

Privacy – Privacy refers to individuals' interests in preventing the inappropriate collection, use, and release of personal information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. Other definitions of privacy include the capacity to be physically left alone (solitude); to be free from physical interference, threat, or unwanted touching (assault, battery); or to avoid being seen or overheard in particular contexts.

Privacy Policy – A privacy policy is a written, published statement that articulates the policy position of an organization on how it handles the personal information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, dissemination, and access. The purpose of the privacy policy is to articulate that the agency/center will adhere to those legal requirements and agency/center policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well-developed and implemented privacy policy uses justice entity resources wisely and effectively; protects the agency, the individual, and the public; and promotes public trust.

Privacy Protection – This is a process of maximizing the protection of privacy, civil rights, and civil liberties when collecting and sharing information in the process of protecting public safety and public health.

Protected Information – Protected information is personal information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and laws of the United States and applicable Rhode Island and tribal constitutions and State of Rhode Island, local, and tribal laws, ordinances, and codes.

Public:

Public includes:

Any person and any for-profit or nonprofit entity, organization, or association; Any governmental entity for which there is no existing specific law authorizing access to the agency's/center's

information; Media organizations; and Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the agency.

Public does not include:

Employees of the agency; people or entities, private or governmental, who assist the agency/center in the operation of the justice information system; and Public agencies whose authority to access information gathered and retained by the agency/center is specified in law.

Public Access – Public access relates to what information can be seen by the public; that is, information whose availability is not subject to privacy interests or rights.

Record – Any item, collection, or grouping of information that includes personally identifiable information and is maintained, collected, used, or disseminated by or for the collecting agency or organization.

Redress – Internal procedures to address complaints from persons regarding protected information about them that is under the agency's/center's control.

Retention – ***(Refer to Storage)***

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

Security – Security refers to the range of administrative, technical, and physical business practices and mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes. Computer and communications security efforts also have the goal of ensuring the accuracy and timely availability of data for the legitimate user set, as well as promoting failure resistance in the electronic systems overall.

Source Agency—Source agency refers to the agency or organizational entity that originates SAR (and when authorized, ISE-SAR) information.

Storage [or Retention]: Refers to the storage and safeguarding of terrorism-related information, to include homeland security information, terrorism information, and law enforcement information relating to terrorism or the security of our homeland by both the originator of the information and any recipient of the information.

Suspicious Activity—Defined in the ISE-SAR Functional Standard (Version 1.5) as "observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity." Examples of suspicious activity include surveillance, photography of sensitive infrastructure facilities, site breach or physical intrusion, cyberattacks, testing of security, etc.

Suspicious Activity Report (SAR)—Official documentation of observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity. Suspicious activity report (SAR) information offers a standardized means for feeding 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.

Terrorism Information – In accordance with Intelligence Reform and Terrorism Prevention Act, as recently amended by the 9/11 Commission Act enacted on August 3, 2007 (P.L. 110-53), the Information Sharing Environment facilitates the sharing of terrorism, including weapons of mass destruction information, and homeland security information, as defined 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 Information Sharing Environment will facilitate the sharing of "terrorism information", as defined in 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 includes intelligence information.

Tips and Leads Information or Data—Generally uncorroborated reports or information generated from inside or outside a law enforcement agency that allege or indicate some form of possible criminal activity. Tips and leads are sometimes referred to as suspicious incident report (SIR), suspicious activity report (SAR), and/or field interview report (FIR) information. However, SAR information should be viewed, at most, as a subcategory of tip or lead data. Tips and leads information does not include incidents that do not have a criminal offense attached or indicated, criminal history records, or CAD data. Tips and leads information should be maintained in a secure system, similar to data that rises to the level of reasonable suspicion.

A tip or lead can come from a variety of sources, including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information may be based on mere suspicion or on a level of suspicion that is less than "reasonable suspicion" and, without further information or analysis, it is unknown whether the information is accurate or useful. Tips and leads information falls between being of little or no use to law enforcement and being extremely valuable depending on the availability of time and resources to determine its meaning.

User—An individual representing a participating agency who is authorized to access or receive and use a center's information and intelligence databases and resources for lawful purposes.

APPENDIX B
(Rhode Island State Police General Order – 77J)

Rhode Island State Police
General Order – 77J
Section
Law Enforcement Operations – Investigations
Rev. 5/15/2009
Article
77 – Types of Investigations
Title
Homeland Security – Fusion Center
Special Instructions

I. PURPOSE

To provide guidelines concerning the establishment and operation of the Rhode Island State Fusion Center.

II. DEFINITIONS

A. FUSION CENTER-An effective and efficient mechanism to exchange information and intelligence, maximize resources, streamline operations, and improve the ability to fight crime and terrorism by merging data from a variety of sources.
B. CRIMINAL INTELLIGENCE-Information collection and analysis conducted to support the anticipated need for decision-making and action.
C. DISSEMINATION-Distribution of information and intelligence in accordance with rules and laws.
D. INFORMATION-unevaluated and untested facts and data obtained from observations, comments, reports, and pictures regarding people, places, things, and events
E. HOMELAND SECURITY-a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur.

F. OPERATION SAFE-RI-A program initiated by the Rhode Island State Fusion Center to foster an exchange of information with the private sector.
G. FEDERAL BUREAU OF INVESTIGATION JOINT TERRORISM TASK FORCE (J.T.T.F.)-a multi-agency task force operated and managed by the Federal Bureau of Investigation to conduct terrorism investigations.

III. POLICY

The Rhode Island State Fusion Center's mission is to facilitate the efficient, timely, and accurate exchange of information between local, state, and federal public safety agencies and private sector organizations. Through a cooperative and coordinated approach, the Rhode
46.3.1
GO – 77J
Page 2 of 4
Rev. 5/15/2009
Island State Fusion Center will augment law enforcement operations by acting as a centralized, comprehensive criminal intelligence center to coordinate the exchange of criminal information on a statewide basis. The Rhode Island State Fusion Center will collect, analyze and disseminate intelligence information in an effort to identify, investigate, and prevent criminal activity relevant to terrorism and public safety. Members assigned to the Fusion Center will also actively investigate all information and leads received that could be associated with terrorist activity or may pose a threat to Homeland Security.

IV. PROCEDURES

A. The Rhode Island State Fusion Center is managed by the Division of State Police and is comprised of State Police Detectives, civilian analysts and representatives from various local law enforcement agencies. A Memorandum of Understanding will be signed by participating agencies assigning personnel to the Fusion Center.
46.3.1
46.3.2
B. The Fusion Center is a component of the Rhode Island State Police Intelligence Unit, which is overseen by the Intelligence Unit Commander.
C. In accordance with Department of Justice reporting requirements, members of the Detective Bureau and Patrol Division shall forward any type of investigative information to the Fusion Center that may be associated with terrorist activity. This communication shall be made in the form of an incident report or e-mail. If the activity needs immediate attention, then notification will be made via telephone call. The notification shall be made in a timely manner following the Division's established policies and procedures relating to chain of command. If the information is obtained outside the hours of operation of the Fusion Center, the Division member's supervisor shall evaluate the information to determine if an imminent threat to public safety exists, requiring immediate notification of a member of the Fusion Center. If immediate notification is necessary, the Intelligence Unit Commander or his designee shall be contacted via the Division's Emergency notification contact list. This reporting requirement does not prohibit members from responding to an actual, ongoing event that requires an immediate law enforcement response to protect the safety of the public. Examples of activity that should be reported to the Rhode Island State Fusion Center that may be associated with terrorist activity includes but is not limited to the following:

1. Surveillance-May include individuals obtaining video footage, still photographs, sketches or diagrams of key facilities or structures, such as train stations, airports, bridges, chemical plants, government buildings, hospitals, public utilities, etc.
2. Elicitation-Attempts to gain sensitive information regarding key facilities or personnel through personal contact, telephone, mail, or e-mail. An example of this activity may include an individual attempting to obtain blue prints of a government building.
GO-77J
Page 3 of 4
Rev. 5/8/07
3. Testing of Security-Attempts to penetrate or test physical security and response procedures at key facilities. Examples of possible testing of security include false building alarms, breaching of physical barriers, running of security gates, etc.
4. Acquiring of Supplies-Attempts to improperly acquire explosives, weapons, ammunition, dangerous chemicals, flight manuals or other materials that could be used in a terrorist attack or suspicious or improper attempts to acquire official vehicles, uniforms, badges, access cards or identifications for key facilities.
5. Suspicious Persons Out of Place-Presence of individuals who do not appear to belong in the specific workplaces, business establishments or key facilities.
6. Dry Run or Trial Run-Behavior which appears to denote planning for terrorist activity such as mapping out routes, playing out scenarios, monitoring key facilities and timing traffic flow or signals.
7. Deploying Assets-Individuals or supplies getting into position to commit a terrorist act. This may include the stockpiling of suspicious materials or abandoning potential containers for explosives to include vehicles, and suitcases.
D. The Rhode Island State Fusion Center is actively engaged in sharing information with members of Federal, State and local law enforcement. The Rhode Island State Fusion Center utilizes various methods of the dissemination of information including Fusion Center bulletins.
E. Prior to the dissemination of any information, the Rhode Island State Fusion Center ensures that the individuals have been properly vetted and have a legitimate need to receive the information. Furthermore, any information being shared electronically will meet all Federal guidelines and standards including 28CFR Part 23 requirements.
F. The Rhode Island State Fusion Center maintains a close working relationship with the Federal Bureau of Investigation Joint Terrorism Task Force. A member of the Rhode Island State Police will be assigned to the FBI Joint Terrorism Task Force and will serve as a liaison between both agencies. *46.3.1*
G. The Rhode Island State Fusion Center also actively engages in sharing information with individuals from the private sector through community outreach programs such as Operation Safe-RI.
H. The Fusion Center will assist other members of law enforcement by maintaining connections a wide array of public, subscription and law enforcement databases.
GO – 77J
Page 4 of 4
Rev. 5/15/2009
I. The Rhode Island State Police Fusion Center provides terrorism awareness
46.3.3

training to members of the Division's In-Service training curriculum, as well to members of local law enforcement training academies. In addition, the Rhode Island State Fusion Center educates private citizens and companies about the role of the Fusion Center and how suspicious activity can be reported. A toll free telephone number will be established to assure individuals can readily contact the Rhode Island State Fusion Center.
By Order of Colonel Doherty
Brendan P. Doherty
Colonel
Superintendent

APPENDIX C
(Rhode Island State Police General Order – 54J)

Rhode Island State Police
General Order – 54J
Section:
Law Enforcement Operations – Field Operations
Rev. 1/21/10
Article:
54 – Records and Reporting
Title:

Rhode Island Law Enforcement Telecommunications System Policy and Procedures

Special Instructions:

I. PURPOSE

To provide enhanced security and accountability in the use of the Rhode Island Law Enforcement Telecommunications System (RILETS).

II. POLICY

The Division of State Police recognizes that the Rhode Island Law Enforcement Telecommunications System must be made safe from unauthorized access while ensuring its use for Official Business only.

III. PROCEDURES

A. Logons and Passwords

1. Every authorized State Police employee will be assigned a unique RILETS User Identification Number and Password by the Technical Services Unit. The RILETS User Identification number and password must be used to access the system.

B. Criminal Record Queries and Interstate Identification Index Queries

1. Each Criminal Record (QR) and/or Interstate Identification Index (QH) query will include the following mandatory fields:

a. Operator Number/Badge Number

b. Case Number/Arrest Number/Complaint Number or Reason/Comments

C. Telephonic Inquiries from Outside Law Enforcement Agencies.

82.1.1a,c

1. Sworn personnel and RILETS Telecommunicators are prohibited from honoring any telephonic requests from outside law enforcement agencies.

GO – 54J

Page 2 of 4

Rev. 1/21/10

2. All requests for RILETS information must be submitted via facsimile on agency letterhead with the proper authorized signature. Responses will be made via facsimile to the requesting agency.

3. All facsimile requests will be forwarded to the Director of RILETS for retention.

D. Monthly Audit of Criminal History Inquiries.

1. The NCIC Control room's RILETS Criminal History inquires will be reviewed by the Director of RILETS and crossed checked against the manual logs on a monthly basis. The Director of RILETS will then forward a memorandum to the Major - Administrative Services certifying if any inconsistencies and/or discrepancies had been found.

E. Manual Log – NCIC

1. When requested by an authorized individual, RILETS Telecommunicators are to ensure that each and every RILETS Criminal History Transaction is properly sent and manually logged with both the RILETS Operator Identification Number, and the Badge Number or assigned Identification Number of the authorized individual requesting the inquiry.

2. These manual logs will be retained by the Director of RILETS.

F. Annual Audit of RILETS Users and Passwords

1. The Director of RILETS shall perform an annual audit for verification of all passwords, access codes, and unauthorized access violations.

2. A report detailing the findings of the annual audit will be submitted to the Major – Administrative Services.

G. RILETS Inquiries
1. All in-house, walk-in, and telephonic inquiries from Division members will be made through the NCIC Telecommunications Center. Other confidential inquiries requiring special processing will be prepared with the approval of the Detective Commander or Assistant Detective Commander.
GO-54J
Page 3 of 4
Rev. 1/21/10
H. Non-Law Enforcement Agencies
1. No RILETS inquiries will be provided to any non-law enforcement agency. If there are any questions about non-law enforcement agency access, they should be forwarded to the Director of RILETS.
2. All non-law enforcement uses of the system must be approved by the Director of RILETS.
I. Criminal History Dissemination Logs
1. A manual log will be created and maintained in Telecommunications that will record each time that a RILETS or NCIC III Criminal History record is printed and given to a member of the State Police. The log will delineate the date, time, operator, name of the individual checked, and the member to whom the record was given.
J. Access to RILETS
1. Access to RILETS shall be limited to the sworn members of the State Police, the Investigators in the Auto Theft Unit, the Supervisors, and members of the Telecommunications Unit, the members of the Technical Services Unit, and support staff in the Criminal Identification, and Commercial Enforcement Units. All access must be for an official purpose and as part of the individual's official duties.
K. Questions and Clarifications
1. All questions and clarifications regarding RILETS, to include access rights, dissemination of information, and policies must be directed to the Director of RILETS.
L. Off-line Searches
1. All requests for off-line searches must be made and approved through the Officer-in-Charge of the Technology and Communication Services Unit.
By Order of Colonel Doherty
Brendan P. Doherty
Colonel
GO – 54J
Page 4 of 4
Rev. 1/21/10
Superintendent

A P P E N D I X D

(Rhode Island State Police General Order – 2D)

Rhode Island State Police
General Order – 2D
Section:
Administration – General Management
Rev. 1/21/10
Article:
2 – Management Reporting
Title:
Records Retention Schedule
Special Instructions:
I. PURPOSE
To establish guidelines for the retention and destruction of Division records as approved by the Secretary of State's Public Records Administration Program.
82.1.3
42.1.3e
42.1.6c
II. POLICY
The Division shall regularly review its records and in those cases in which records are no longer needed, the below procedures are to be followed for destruction. The approved Rhode Island State Police Records Retention Schedule, the Statewide Records Retention Schedule for General Office Administrative, Fiscal and Retention Records entitled, General Schedule #1 and a Statewide Records Retention Schedule for Personnel and Payroll Records entitled, General Schedule #2, will all be located with each of the twelve official copies of the written directives and contain the required minimum time periods that records must be retained prior to seeking approval from the State Archives to destroy.
III. DEFINITIONS
A. Designated Record Custodian – the Detective Commander for the Detective Bureau, the District Commanders for the Patrol Bureau and all units reporting to the District Commanders and the Major – Administrative Services for all other units.
B. Certificate of Records Destruction form – a form listing records to be destroyed that classifies the records according to the Records Retention Schedules approved by the Secretary of State Public Records Administration program.
IV. PROCEDURES
A. Review
1. Records should be periodically reviewed by each Barracks/Bureau/Unit Supervisor and disposed of in accordance with the respective records destruction schedule and procedures. This review should normally occur during July and August of each year, subject to availability of personnel to facilitate a routine destruction schedule.
GO – 2D
Page 2 of 4
Rev. 1/21/10

2. If personnel levels permit additional periods of review, records may be reviewed and the Certification of Records Destruction forms prepared on a more frequent basis.
3. Records should not be listed on a records destruction schedule if they are the subject of any pending litigation or current public records request. To determine if any of the records are the subject of civil litigation, the proposed list should be forwarded to Legal Counsel for review prior to forwarding to the Designated Records Custodian.
B. Completion of Certificate of Records Destruction Form
1. Once a review is completed and the applicable records have been identified, a "Certification of Records Destruction" form should be completed with the following information:
a. Department -- "Rhode Island State Police."
b. Division -- Insert particular Barracks/Bureau/Unit.
c. Date -- Enter the date the form is prepared.
d. Record Series Number -- Enter the exact series number from the Records Retention Schedule -- for example: SP-1.2 for Barracks Incident Files.
e. Record Series Title -- Enter the exact series title from the Records Retention Schedule. If the Barracks/Bureau/Unit uses a different series title than found in the schedule, insert the Barracks/Bureau/Unit title in brackets "[ ]."
f. Dates To/From -- Enter the earliest and latest dates covered by the records proposed for destruction. In most cases, just the year will be sufficient. NOTE: If the retention period of a particular series is qualified by wording such as "successful audit plus one year," or "three years after expiration of statute of limitations," the year of expiration must be noted.
g. Volume -- Enter the volume of records to be destroyed. Volume is most easily measured by the number of inches of linear feet of records, although cubic foot measurements give a more accurate figure. A "Table of Volume" and a cubic foot equivalency formula provided by the State Archives is enclosed.
h. The completed form will be reviewed and signed by the barracks/bureau/unit supervisor or Records Custodian.
GO-2D
Page 3 of 4
Rev. 11/21/10
C. The Records Custodian will forward the signed form to the State Archivist and Public Records Administrator for verification that the records listed on the form are eligible for destruction pursuant to the applicable records retention schedules. Upon verification, the State Archivist and Public Records Administrator will sign and return the Certificate of Records Destruction form to the designated Records Custodian.
D. The designated Records Custodian will then forward the signed Certificate of Records Destruction form to the requesting barracks/unit supervisor.
E. Destruction
1. After receiving the signed Certificate of Records Destruction form that records can be destroyed, the barracks/unit supervisor shall either:
a. Destroy the records by shredding;
b. In the case of a substantial volume of records, the Fleet/Supply Administrator shall be contacted to arrange for a mobile records destruction contractor to shred the records.
F. Retention of Certification of Records Destruction forms

Once the records have been destroyed, the Certification of Records Destruction forms shall be forwarded to the Division's Legal Counsel for permanent retention as the legal replacement for those records.
By Order of Colonel Doherty
Brendan P. Doherty
Colonel
Superintendent
GO – 2D
Page 4 of 4
Rev. 1/21/10