South Carolina Information and Intelligence Center (SCIIC)

Privacy, Civil Rights, and Civil Liberties Protection Policy

A. Purpose Statement

1. The purpose of this Privacy, Civil Rights, and Civil Liberties Protection Policy (hereafter "P/CRCL Policy") is to promote conduct by the SC Information and Intelligence Center (hereafter "SCIIC"), source agencies, and user agencies (hereafter collectively referred to as "participating agencies" or "participants") that complies with the U.S. Constitution, the Privacy Act of 1974 as amended, 28 CFR Part 23 and all other applicable federal, state, local, and tribal laws, regulations, and policies (See Appendix B, Applicable Laws Relevant to Privacy, Civil Rights, and Civil Liberties). This P/CRCL Policy also assists participants in:

- Protecting individual privacy, civil rights, civil liberties, and other protected interests.
- Increasing public safety and improving national security.
- Protecting the integrity of systems for the observation and reporting of terrorism-related criminal activity and information.
- Encouraging individuals or community groups to trust and cooperate with the justice system.
- Promoting governmental legitimacy and accountability.
- Making the most effective use of public resources allocated to public safety agencies.

2. The SCIIC is a collaborative effort to provide resources, expertise, intelligence and information analysis and products to state, local and tribal law enforcement personnel, first responders and the citizens, businesses and critical infrastructure enterprises of South Carolina with the goal of maximizing the ability to detect, prevent, apprehend and respond to criminal and terrorist activity. In doing so, the SCIIC collects, evaluates, analyzes, and disseminates information and intelligence data (records) regarding criminal and terrorist activity in the state while protecting privacy, civil rights, civil liberties and other protected interests. This includes implementing appropriate privacy and civil liberties safeguards as outlined in the principles of the Privacy Act of 1974, as amended, to ensure that the information privacy and other legal rights of individuals and organizations are protected.

3. The South Carolina Law Enforcement Division (SLED) SCIIC was established under South Carolina Governor's Executive Order 2003-02 (January 17, 2003) to provide the information sharing and exchange of terrorism and crime-related information among members of the law enforcement community, corrections, public safety, public health, and critical infrastructure communities of South Carolina. The focus of the SCIIC is to combine the intelligence and information sharing efforts of all participating agencies to enhance the ability to predict, prevent, and respond to unlawful activity and threats to our nation and state. This is a process whereby information is collected, integrated, evaluated, analyzed, and disseminated through established procedures for law enforcement purposes and in the interest of public safety. The intelligence products and services are made available to law enforcement agencies, public safety agencies, principals of critical infrastructure and key resources, and other entities contributing to public safety throughout the state and country.

4. The following records are subject to the P/CRCL Policy and the guidelines dealing with (U//FOUO) use only. They are not subject to the requirements of 28 CFR Part 23 due to the fact that they are not considered criminal intelligence files. Applicable sections are marked (Applicability: All).

a. Research files (open source documents, bulletins, advisories, and assessments by others)
b. Criminal history files (including but not limited to SCIEx, NCIC, SC Department of Corrections information and SC Department of Probation, Parole and Pardon information)
c. Law Enforcement assistance requests, case management records, and support files (consists of working documents compiled in response to requests by supported agencies, temporary storage of results of criminal history database queries, reports from case agents, etc.)
d. Tips and Leads files.

5. The following records are considered criminal intelligence files (CI Files) and are subject to the P/CRCL Policy, as well as the additional requirements found in 28 CFR Part 23, and ISE Privacy Guidelines ("Protected Personal Information").

a. GangNet
b. CrimeNtel

B. Policy Applicability and Legal Compliance (Applicability: All)

1. This policy applies to all persons who access SCIIC databases which include personally identifiable information (PII) and to all organizations which enter into memoranda of agreement/understanding with the SCIIC for exchange of PII. 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. All persons provided direct access to SCIIC record systems will be provided a copy of this policy in printed or electronic form and briefed on privacy policies and their obligations there under in the collection, use, analysis, retention, destruction, sharing, and disclosure of information, and will receive privacy, civil rights, and civil liberties training. A signed statement acknowledging this briefing and awareness of the penalties in accordance with SLED policy and state law for violations thereof will be maintained.

2. The SCIIC will provide a soft copy of its P/CRCL Policy to all SCIIC personnel. A soft copy or printed copy will be provided to non-agency personnel who provide services to the SCIIC and to each source agency and SCIIC authorized user and will require both a written acknowledgement of receipt of this policy and a written agreement to comply with applicable provisions of this policy. This policy applies to all persons who access SCIIC databases which include personally identifiable information and to all organizations which enter into memoranda of agreement/understanding with the SCIIC for exchange of PII. The policy will also be publicly

available on the website for public assurance and acknowledgment of the public's right to privacy.

3. All SCIIC personnel, participating agency personnel, personnel providing information technology services to the agency, private contractors, and other authorized users shall comply with applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to the U.S. Constitution, the Privacy Act of 1974, as amended, and state, local, and federal privacy, civil rights, civil liberties legal requirements applicable to the SCIIC and/or other participating agencies. The applicable legal requirements are attached as Appendix B to this Policy.

4. This is the SCIIC internal operating policy to ensure compliance with applicable laws protecting privacy, civil rights, and civil liberties.

C. Governance and Oversight (Applicability: All)

1. The Director of the SCIIC will have primary responsibility for operating the SCIIC, ISE- SAR information system operations, and coordinating personnel involved with the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing or disclosure of information, and enforcing the provisions of this policy.

2. The Fusion Center Advisory Group consists of individuals appointed by the Chief of SLED and the Director of the SCIIC to provide broad oversight of SCIIC policies and to advise the senior leadership on matters concerning the SCIIC and its interactions with law enforcement, homeland security, critical infrastructure enterprises, and the public.

3. The SCIIC Privacy Officer will support the Fusion Center Advisory Group on privacy, civil rights, and civil liberties related issues and is appointed by the Director of the SCIIC. The SCIIC Privacy Officer will review the P/CRCL Policy annually and make recommendations for changes as necessary to the SCIIC Director. The SCIIC Privacy Officer receives reports regarding alleged errors and violations of the provisions of this policy, receives and coordinates complaint resolution under the center's redress policy, and serves as the liaison for the Information Sharing Environment, ensuring that privacy protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy- enhancing technologies. The SCIIC Privacy Officer can be contacted at the following address: privacyofficer@sled.sc.gov.

4. The SCIIC's Privacy Officer will be trained in privacy, civil rights, and civil liberties issues, the requirements of this policy and will ensure that the center adheres to the provisions of these Privacy Guidelines and other requirements for participation. The SCIIC Privacy Officer will respond to all reports of errors and violations and ensure that enforcement procedures and sanctions outlined in section N.3, Enforcement, are adequate and enforced.

D. Definitions (Applicability: All)

The primary terms and definitions used in this P/CRCL Policy are set forth in Appendix A, Terms and Definitions.

E. Criminal Intelligence Information

1. (Applicability: CI Files) The SCIIC will seek or retain criminal intelligence information, tip/lead/SAR/ISE-SAR information, and other information or intelligence which a source agency (the SCIIC or other agency) has determined constitutes "suspicious activity" and which:

- Is based, on (a) a criminal predicate or (b) a possible threat to public safety, including potential terrorism-related conduct; or
- 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
- 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
- Is useful in crime analysis or in the administration of justice and public safety (including topical searches); and
- The source of the information is reliable and verifiable or limitations on the quality of the information are identified; and
- The information was collected in a fair and lawful manner, with the knowledge and consent of the individual, if appropriate.

(Applicability: CI Files) The SCIIC may retain 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. (Applicability: CI Files) The SCIIC will not seek or retain, and information-originating agencies will agree not to submit, 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 lawful event; or their races, ethnicities, citizenship, national origin, ages, disabilities, genders, gender identities or sexual orientations.

3. (Applicability: CI Files) The SCIIC applies labels to center-originated information by dataset to indicate to the accessing authorized user that:

- The information is protected information (as defined by the center to include personal information on any individual) [see definitions of "protected information" and "personal information" in Appendix A of policy], and, to the extent expressly provided in this policy, includes organizational entities.
- The information is subject to state and federal laws restricting access, use or disclosure.

4. (Applicability: CI Files) Upon receipt of tips, leads, SARs, or other information for which the SCIIC is the initial point of entry into a SCIIC file, SCIIC personnel will assess the information to determine or review its nature, usability, and quality. Personnel will assign categories to the information (or ensure that the originating agency will assign categories to the information) and label the information to reflect the assessment, such as:

- Whether the information consists of tips and leads data, suspicious activity reports, criminal history or intelligence information, case records, conditions of supervision, case progress, or other information category.;
- The source of the information sought and collected;
- The nature of the source as it affects veracity (for example, anonymous tip, trained interviewer or investigator, public record, private sector);
- The reliability of the source (for example, reliable, usually reliable, unreliable, unknown);
- The validity of the content (for example, confirmed, probable, doubtful, cannot be judged);
- Whether there are any restrictions on retention or release of the information and if so, the specific restrictions;
- The results of this vetting process will be recorded with the data.

5. (Applicability: CI Files) At the time a decision is made to retain information, SCIIC personnel will ensure that the information is labeled, to the maximum extent feasible and consistent with applicable limitations on access and to reflect any limitations on disclosure based on sensitivity of disclosure (dissemination description code), in order to:

- Protect an individual's right of privacy, civil rights, and civil liberties.
- Protect confidential sources and police undercover techniques and methods.
- Not interfere with or compromise pending criminal investigations.
- Provide any legally required protections based on an 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.

6. (Applicability: CI Files) The labels applied to existing information will be reevaluated whenever:

- New information is added that has an impact on access limitations, confidence, or the sensitivity of disclosure of the information; or
- There is a change in the use of the information affecting access or disclosure limitations; for example, the information becomes part of court proceedings for which there are different public access laws.

7. SCIIC personnel will 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:

- (Applicability: All) Make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources of information; accurate; current; complete, including the relevant context in which it was sought or received and other related information; and merged with other information about the same individual or organization only when the applicable standard has been met.
- (Applicability: CI Files) Prior to either allowing access to or dissemination of tips and leads or SAR information or entering personally identifiable information into a criminal

intelligence file, 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 results of this vetting process will be recorded with the data. The SCIIC will use a standard reporting format and data collection codes for SAR information.

- (Applicability: All) Store the information using the same storage method used for data that rises to the level of reasonable suspicion
- (Applicability: CI Files) Include an audit and inspection process, supporting documentation, and labeling of the data by dataset to delineate it from other information.
- (Applicability: All) Allow access to or disseminate the information using the same 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).
- (Applicability: All) 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.
- (Applicability: CI Files) Retain information for up to five years to work a tip or lead or SAR information to determine its credibility and value, assign a "disposition" label (for example, undetermined or unresolved, cleared or unfounded, or under active investigation) so that a subsequently authorized user knows that status and purpose for the retention and will retain the information based on the retention period associated with the disposition label.
- (Applicability: All) Adhere to and follow the center's physical, administrative, and technical security measures that are in place for the protection and security of tips and leads information. Tips, leads, and SAR information will be secured in a system that is the same or similar to the system that secures data that rises to the level of reasonable suspicion.

8. (Applicability: All) The SCIIC will incorporate the gathering, processing, reporting, analyzing, and sharing of SAR information 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 the privacy, civil rights, and civil liberties of individuals.

9. (Applicability: CI Files) The SCIIC will provide notice through data field labels or narrative information to enable authorized users to determine the nature of the protected information in the shared space and how to handle the information in accordance with applicable legal requirements, including any restrictions based on information security or classification.

(Applicability: CI Files) 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.

10. (Applicability: CI Files) The SCIIC requires certain basic descriptive information to be entered and electronically associated with the 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 that will be recorded include:

- The name of the originating agency, department, component, and subcomponent (where applicable).
- If applicable, the name of the agency's justice information system from which the information is disseminated.
- The date the information was collected (submitted) and, where feasible, the date its accuracy was last verified.
- The title and contact information for the person to whom questions regarding the information, including its accuracy, should be directed.
- The date the information was entered and reviewed; the date by which the information must be validated or purged.

11. (Applicability: CI Files) The SCIIC 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.

- Criminal Intelligence Files will include a statement on at least the initial computer screen that the records contained therein are subject to 28 CFR Part 23.
- Reports generated from Criminal Intelligence Files will include a statement that the information is subject to 28 CFR Part 23. Hard copy files will include "Protected Personal Information" on the file cover. "Protected information" is defined in Appendix A of the policy.

12. (Applicability: CI Files) The SCIIC will keep a record of the source of all information sought and collected by the center.

F. Acquiring and Receiving Information

1. Information acquisition, access, and investigative techniques used by the SCIIC and information-originating agencies must comply with and adhere to applicable law, regulations, and guidelines, including, where applicable, U.S. and state constitutional provisions, applicable federal and state law provisions, local ordinances, and regulations. These include, but are not limited to:

- United States Constitution and Amendments I-XXVII;
- The Privacy Act of 1974 (5 U.S.C. 552a);
- United States Executive Order 12958 "Classified National Security Information";
- United States Department of Justice Criminal Intelligence Systems Operating Policies; 28 CFR Part 23
- SC Freedom of Information Act, SC Code Ann. §§30-4-10 et seq.;
- SC Code Ann. §39-1-90;
- Consumer Protection Code, SC Code Ann. §37-20-110 et seq.;
- SC Code Ann. Regulations 73-20 and 73-30;

- Intelligence Reform and Terrorism Prevention Act of 2004: 118 STAT. 3666; P.L. 108-458 Section 1016;
- 6 USC §485;
- Snakenberg v. Hartford Cas. Ins., 299 S.C. 164, 383 S.E.2d 2 (Ct. App. 1989);
- State v. Houey; 375 SC 106, 651 SE2d 314 (2007);
- SLED Policy 9.6;
- SCIIC Security Policy.

Appendix B includes a detailed discussion of SC case law and its application to the SCIIC and laws relevant to seeking, retaining, or disseminating information at the state and federal level.

2. (Applicability: CI Files) The SCIIC'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 other personnel at the SCIIC and source agencies who acquire SAR information that may be shared with the SCIIC will be trained to recognize behavior that is indicative of criminal activity related to terrorism.

3. (Applicability: CI Files) The SCIIC's SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved 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 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. (Applicability: CI Files) When a choice of investigative techniques is available, information documented as a SAR should be acquired or investigated using the least intrusive feasible means, taking into account such factors as the effect on individuals' privacy and potential damage to reputation.

5. All external agencies that access the SCIIC's information or share information with the center are governed by the laws and rules governing those individual agencies, including applicable federal and state laws.

6. (Applicability: All) The SCIIC will contract only with commercial database entities that provide an assurance that they gather personally identifiable information in compliance with local, state, and federal laws and which is not based on misleading information collection practices.

7. (Applicability: CI Files) The SCIIC will not directly or indirectly receive, seek, accept, or retain information from:
- An individual or nongovernmental information provider who may or may not receive a benefit for providing the information, except as expressly authorized by law or center policy;

- An information provider who is legally prohibited from obtaining or disclosing the information; or
- A source that used prohibited means to gather the information.

G. Information Quality Assurance

1. (Applicability: CI Files) The SCIIC will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources of information; accurate; current; complete, including the relevant context in which it was sought or received and other related information; and merged with other information about the same individual or organization only when the applicable standard has been met.

2. (Applicability: CI Files) At the time of retention in the system of tips, leads, SARs, or other information for which SCIIC is the initial point of entry into a SCIIC file, SCIIC personnel will assess the information to determine or review its nature, usability, and quality. Personnel will assign categories to the information (or ensure that the originating agency will assign categories to the information) and label the information to reflect its level of quality (accuracy, completeness, currency, and confidence [verifiability and reliability]).

3. (Applicability: All) The SCIIC will investigate, in a timely manner, alleged errors and deficiencies and will correct, delete, or refrain from using protected information found to be erroneous or deficient. SCIIC personnel will take reasonable measures to ensure that information entered into SCIIC record systems is accurately transcribed. Information compiled by SCIIC personnel from agents' reports, public or private records, open sources, will be vetted for accuracy and consistency.

4. (Applicability: CI Files) The labeling of retained information will be reevaluated when new information is gathered that has an impact on the center's confidence in the validity or reliability of the retained information.

5. (Applicability: CI Files) The SCIIC will conduct periodic data quality review of information for which the SCIIC is the office of primary responsibility and make every reasonable effort to ensure that the information will be corrected or deleted from the system, or not used when the center identifies the information that is erroneous, misleading, obsolete, or otherwise unreliable.

6. (Applicability: CI Files) Originating agencies external to the SCIIC are responsible for reviewing the quality and accuracy of the data provided to the center. The SCIIC will notify the originating agency or the originating agency's privacy officer, in writing or electronically, when the center reviews the quality of the information it has received from an originating agency and identifies data that may be inaccurate or incomplete, 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.

7. (Applicability: CI Files) The SCIIC will use written or electronic notification to inform recipient agencies when information previously provided to the recipient agency is deleted or

changed by the center because the information is erroneous. The circumstances of the changes will be recorded in the same system; the database of requests involving that information will be reviewed and any officials or agencies which have previously been provided the edited information will be notified of the changes. However, nothing herein shall be construed to require that each recipient of a bulletin or advisory which included the changed information must be notified; a correction broadcast by the same means as the original bulletin or advisory will suffice.

H. Collation and Analysis

1. (Applicability: CI Files) The SCIIC will ensure that each analyst authorized to access criminal intelligence files receives training on analysis of criminal intelligence information acquired or accessed by the center and has successfully completed a background investigation and has appropriate security clearance, if applicable. Access to SCIIC records will be provided to individuals who are hired by SLED or a participating agency for a position in the SCIIC; users of participating agencies; and, contractors employed by SLED providing services the SCIIC.

2. (Applicability: CI Files) Information subject to collation and analysis is information as defined and identified in Section E, Information, paragraph 1.

3. (Applicability: CI Files) Information acquired or received by the SCIIC or accessed from other sources is analyzed according to priorities and needs, including analysis to:

- Further terrorism prevention, investigation, force deployment, or prosecution objectives and priorities established by the SCIIC.
- Provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in terrorism- related activities.

The SCIIC requires that all analytical products be reviewed by a supervisor or the privacy officer, as appropriate, prior to dissemination or sharing by the center to ensure that they provide appropriate privacy, civil rights, and civil liberties protections.

I. Merging Records

1. (Applicability: CI Files) Records 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. The set of identifying information sufficient to allow merging includes but is not limited to: name (full, partial, or street name); date of birth; law enforcement, corrections system, or Federal database identifying number; individual identifiers such as fingerprints, photographs, physical description, height, weight, eye and hair color, race, ethnicity, tattoos, scars, DNA, retinal scan, or facial recognition; social security number; driver's license or state identification card number; in the case of organizations, the set of identifying information includes but is not limited to: name or names; address; leadership; membership; federal or state tax ID number; telephone number; URL or email address.

2. (Applicability: CI Files) If the matching requirements are not fully met but there is an identified partial match, the information may be associated if accompanied by a clear statement that it has not been conclusively established that the information belongs to the same individual or organization.

J. Sharing and Disclosure

1. (Applicability: All) Credentialed, role-based access criteria will be used by the SCIIC, as appropriate, to control:

- The information to which a particular group or class of users can have access based on the group or class.
- The information a class of users can add, change, delete, or print.
- To whom, individually, the information can be disclosed and under what circumstances.

For purposes of this paragraph, "credentialed" means completion of all required screening and training and written authorization to access specific databases. It is not synonymous with law enforcement "credentialing" and does not imply that only credentialed or sworn officers may access databases subject to this policy.

2. (Applicability: CI Files) As a matter of protocol, the SCIIC provides all SARs to the Federal Bureau of Investigation Joint Terrorism Task Force. Should the SCIIC provide SAR information directly to the NSI, adherence to the current version of the ISE-SAR Functional Standard for its SAR process, including the use of a standard reporting format, NSI-approved data collection codes, and ISE-SAR information sharing and disclosure business rules for suspicious activity potentially related to terrorism will be required.

3. (Applicability: CI Files) Information retained by the SCIIC and entered into CI Files will be accessed by or disseminated only to persons within the SCIIC 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 law and procedures applicable to the agency for which the person is working. Access and disclosure of personal information will only be allowed to agencies and individual users for legitimate law enforcement and public protection purposes and only for the performance of official duties in accordance with law. An audit trail sufficient to allow the identification of each individual who accessed information retained by the center and the nature of the information access will be kept by the center.

4. (Applicability: CI Files) Agencies external to the SCIIC may not disseminate CI File information accessed or disseminated from the center without approval from the center or other originator of the information.

5. (Applicability: CI Files) Records, information and analyses based on information derived from SCIIC records and databases and retained by the SCIIC will be disseminated to those responsible for public protection, public safety, or public health. Disclosure will be subject to the procedural safeguards of this policy. Disclosure on a proactive basis will be reviewed by a SCIIC

supervisor prior to disclosure. Information from criminal intelligence information databases will be accompanied by a prohibition against subsequent/further disclosure without prior approval of the contributing agency. An audit trail sufficient to allow the identification of each individual who accessed or received information retained by the center and the nature of the information accessed will be kept by the center.

6. (Applicability: All) Searches of SCIIC records or databases based on personally identifiable information or which return personally identifiable information will only be performed for specific official purposes by persons authorized by law to have such access and for only those uses and purposes specified within the law. "Official purposes" may include official requests for assistance from law enforcement or other governmental officials; persons performing such searches will take reasonable steps to verify the identity of requesting officials and will document the identity and contact information for each search. A record identifying each individual who requested, accessed, or received information retained by the center; and the nature of the information requested, accessed, or received; and the specific purpose will be kept for a minimum of two years by the center.

7. (Applicability: All) Information gathered or collected and records retained by the SCIIC may be accessed or disclosed to a member of the public only if the information is defined by law to be a public record or otherwise appropriate for release. A record identifying each individual member of the public who accessed or received information retained by the center and the nature of the information accessed will be kept by the center.

8. (Applicability: All) Information gathered or collected and records retained by the SCIIC will not be:

- Sold, published, exchanged, or disclosed for commercial purposes
- 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
- Disseminated to persons not authorized to access or use the information

9. (Applicability: All) In accordance with SC Code Ann. §30-4-40, the existence, content, and source of the information will not be provided to the public when:

- Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution;
- Disclosure would endanger the health or safety of an individual, organization, or community;
- The information is of a personal nature where the public disclosure thereof would constitute unreasonable invasion of personal privacy;
- The information is a record of a law enforcement and public safety agency not otherwise available by state and federal law that was compiled in the process of detecting and investigating crime if the disclosure of the information would harm the agency by:
    - disclosing identity of informants not otherwise known;
    - prematurely releasing information to be used in a prospective law enforcement action;
    - disclosing investigatory techniques not otherwise known outside the government;
    - endangering the life, health, or property of any person; or,

- disclosing any contents of intercepted wire, oral, or electronic communications not otherwise disclosed during a trial.

- The information source does not reside with the SCIIC;
- The SCIIC does not have a right to disclose information originating with another agency pursuant to a federal requirement.

10. (Applicability: All) The SCIIC will not confirm the existence or nonexistence of information to persons or organizations ineligible to receive the information itself unless otherwise required by law.

K. Redress

K.1 Disclosure

1. (Applicability: All) Upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity and subject to the conditions specified in (J.9), below, an individual is entitled to know the existence of and to review the information about him or her that has been gathered and retained by the SCIIC. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information. The SCIIC's response to the request for information will be made within thirty working days, excepting Saturdays, Sundays, and legal public holidays, and in a form that is readily intelligible to the individual. A record will be kept of all requests and of what information is disclosed to an individual.

2. (Applicability: All) The existence, content, and source of the information will not be made available by the SCIIC to an individual when, under applicable law and court decisions:

- Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution;
- Disclosure would endanger the health or safety of an individual, organization, or community;
- The information is a criminal intelligence information system subject to 28 CFR Part 23;
- No statute or regulation requires its disclosure; or
- The SCIIC or user agency did not originate or does not otherwise have a right to disclose the information.

(Applicability: All) If the information does not originate with the center, the requestor will be referred to the originating agency, if appropriate or required, or the center will notify the source agency of the request and its determination that the disclosure by the center or referral of the requestor to the source agency was neither required nor appropriate under applicable law.

K.2 Corrections

1. (Applicability: CI Files) If an individual requests correction of information originating with the SCIIC that has been disclosed, the SCIIC's Privacy Officer or designee will inform the individual of the procedure for submitting complaints or requesting corrections. A record will be kept of all complaints and requests for corrections and the resulting action, if any.

K.3 Appeals

1. (Applicability: CI Files) The individual to whom information has been disclosed will be given reasons if requests for correction(s) are denied by the SCIIC, originating agency, or the ISE participating agency. The individual will also be informed of the procedure for appeal when the SCIIC, originating agency, or ISE participating agency has declined to correct challenged information to the satisfaction of the individual to whom the information relates. Challenges to denial of Freedom of Information Act requests is by petition to the Circuit Court for declaratory judgment or injunctive relief in accordance with SC Code Ann. § 30-4-100.

K.4 Complaints

1. (Applicability: CI Files) If an individual has complaints or objections to the accuracy or completeness of protected information that has not been disclosed to him or her that: allegedly has resulted in demonstrable harm to the complainant; is exempt from disclosure; and is shared through the ISE, the SCIIC's Privacy Officer will ensure that the individual is provided with complaint submission or corrections procedures, if necessary. Complaints will be received by the SCIIC's Privacy Officer at the following address: privacyofficer@sled.sc.gov. The Privacy Officer 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. The SCIIC 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 SCIIC will not share the information until such time as the complaint has been resolved. A record will be kept by the SCIIC of all complaints and the resulting action taken in response to the complaint.

2. (Applicability: CI Files) To delineate protected information shared through the ISE from other data, the SCIIC maintains records whereby the source (or originating agency, including ISE participating agencies) is identified within the information.

L. Security Safeguards

1. (Applicability: All) SLED has an Information Security Officer (ISO) designated by the Chief of SLED.

2. (Applicability: All) a. The SCIIC will operate in a secure facility protected from external intrusion. The center will utilize secure internal and external safeguards against network intrusions.

(Applicability: CI Files) b. Access to the center's CI databases from outside the facility will be allowed only over secure networks.

3. (Applicability: CI Files) The SCIIC will secure tips, leads, and SAR information using the same storage method used for data that rises to the level of reasonable suspicion and includes an audit and inspection process, supporting documentation, and labeling of the data by dataset to delineate it from other information.

4. (Applicability: CI Files) The SCIIC will secure CI database information, including tips, leads, and SAR information in the SCIIC's shared space, in a manner such that it cannot be added to, modified, accessed, destroyed, or purged except by SCIIC personnel authorized to take such actions.

5. (Applicability: CI Files) Access to CI Files will be granted only to SCIIC personnel whose positions and job duties require such access and approved and authorized users from participating agencies who have been selected, approved, and trained accordingly.

6. (Applicability: CI Files) Queries made to the SCIIC's data applications will be logged into the data system identifying the user initiating the query.

7. (Applicability: CI Files) The SCIIC will utilize watch logs to maintain audit trails of requested and disseminated information.

8. (Applicability: All) To prevent public records disclosure, risk and vulnerability assessments will not be stored with publicly available data.

9. (Applicability: All) A suspected or confirmed breach of PII will be reported to the SCIIC Director who will coordinate with SLED's ISO as necessary. The SCIIC will follow the data breach notification set forth in SC Code Ann. §1-11-490, Breach of Security of State Agency Data. To the extent allowed by the SC Code Ann. §1-11-490, the SCIIC will immediately notify the originating agency from which the center received personal information of a suspected or confirmed breach of such information.

M. Information Retention and Destruction

1. (Applicability: As stated) Retention of criminal history records is governed by Titles 16, 22, and 23 of the South Carolina Code of Laws. All criminal intelligence information, tips, leads, SARs, and ISE-SARs, will be reviewed for record retention (validation or purge) at least every five (5) years, as provided by 28 CFR Part 23.

2. (Applicability: CI Files) When information has no further value or meets the criteria for removal according to the SCIIC's retention and destruction policy it will be purged, destroyed, and deleted.

3. (Applicability: CI Files) The SCIIC will delete criminal intelligence information or return it to the originating agency once its retention period has expired as provided by this policy unless it is validated as specified in 28 CFR Part 23. The approval of the originating agency is not required.

4. (Applicability: CI Files) A record of information to be reviewed for retention will be maintained by the SCIIC so that appropriate notice of required review and validation or purge will be given.

N. Accountability and Enforcement

N.1 Information System Transparency

1. (Applicability: All) The SCIIC will be open with the public in regard to information and intelligence policies and practices. The SCIIC will make the SCIIC's Privacy, Civil Rights, and Civil Liberties Protection Policy available on the SLED website at www.sled.sc.gov.

2. (Applicability: All) The SCIIC's Privacy Officer will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s) maintained or accessed by the center. The SCIIC Privacy Officer can be contacted at privacyofficer@sled.sc.gov

N. 2 Accountability

1. (Applicability: CI Files) The audit log of queries for information made to the SCIIC will identify the user initiating the query.

2. (Applicability: CI Files) The SCIIC will have access to an audit trail of inquiries to and information disseminated from SCIIC's CI databases, including the ISE-SAR shared spaces. An audit trail will be kept for a minimum of 5 years of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.

(Applicability: CI Files) The SCIIC will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of its users with system requirements and with the provision of this policy and applicable law. This will include logging access to these systems and periodic auditing of these systems so as not to establish a pattern of audits. These audits will be mandated at least annually and a record of the audits will be maintained by the SCIIC Privacy Officer or SCIIC Director designated personnel.

Appropriate elements of this audit and process and key audit outcomes will be complied into a report and may be provided to command staff and oversight entities or governance boards.

3. (Applicability: CI Files) SCIIC personnel shall report errors, violations or suspected violations of the SCIIC's P/CRCL Policy to the SCIIC's Privacy Officer.

4. (Applicability: CI Files) The SCIIC will conduct annual audit and inspection of the information contained in its information systems. The audit will be conducted by designated SCIIC personnel. These personnel have the option of conducting a random audit, without announcement,

at any time without prior notice to the SCIIC. The audits will be conducted in such a manner so as to protect the confidentiality, sensitivity, and privacy of the center's criminal intelligence system. Audit personnel will submit a report of the findings to the Director of the SCIIC.

5. (Applicability: CI Files) The SCIIC's appointed and trained SCIIC Privacy Officer will review the SCIIC's P/CRCL Policy annually and will make appropriate changes in response to changes in applicable law, technology, policy determinations, the purpose and use of the information systems, and public expectations. The SCIIC Privacy Officer may take advice and recommendations from other expert individuals or groups designated by the SCIIC Director into account as part of this review.

N.3 Enforcement

1. (Applicability: All) If the SCIIC receives information that SCIIC personnel, a participating agency, or an authorized user is in noncompliance with the provisions of this policy regarding the gathering, collection, use, retention, destruction, sharing, classification, or disclosure of information, the Director of the SCIIC will:

- Initiate an investigation into the report to determine if the SCIIC personnel, a participating agency, or an authorized user was in noncompliance.

(Applicability: All) If SCIIC personnel are found to be in noncompliance, the Director of the SCIIC will:

- Suspend or discontinue access to information by the personnel, if necessary, until a determination regarding appropriate disciplinary measures, if any, is made;
- Undertake one or more of the following actions as appropriate:
    - Suspend, demote, transfer, or terminate center personnel, as permitted by applicable personnel policies
    - Apply administrative actions or sanctions as provided by SLED rules and regulations or as provided in SCIIC policies
    - Refer the matter to appropriate authorities for criminal prosecution, as necessary.

(Applicability: All) If a participating agency is found to be in noncompliance, the SCIIC will undertake one or more of the following actions as appropriate:

- Request that the relevant agency, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions
- Suspend participating agency access or terminate the MOU, if necessary based on the severity of the noncompliance; and,
- Refer the matter to appropriate authorities for criminal prosecution, as necessary

(Applicability: All) If an authorized user is found to be in noncompliance, the SCIIC will undertake one or more of the following actions as appropriate:

- Suspend or discontinue access to information by the authorized user, if necessary, until a determination regarding appropriate disciplinary measures, if any, is made by the employing agency under any applicable civil service rules or other state or federal laws or regulations regarding the authorized user's employment;

- Assist the appropriate agency with any disciplinary actions and/or hearings as may be necessary; and,
- Refer the matter to appropriate authorities for criminal prosecution, as necessary.

2. (Applicability: All) The SCIIC reserves the right to suspend or withhold service to any of its user agencies or authorized user agency personnel violating this P/CRCL Policy. The SCIIC further reserves the right to deny access to its participating agencies (source or user) that fail to comply with the applicable restrictions and limitations of the SCIIC's P/CRCL Policy.

O. Training

1. The SCIIC will require the following individuals to participate in training programs regarding implementation of and adherence to this P/CRCL Policy:

- All assigned personnel of the SCIIC.
- Personnel providing information technology services to the SCIIC.
- Staff in other public agencies or private contractors providing information technology or related services to the SCIIC.
- Source agency personnel providing organizational processing services for SAR information submitted to the SCIIC.
- User agency personnel and individuals authorized to access SCIIC information who are not employed by the SCIIC or a contractor.

2. The SCIIC will provide special training regarding the SCIIC's requirements and policies for collection, use, and disclosure of protected information to personnel authorized to share protected information through the Information Sharing Environment (ISE).

3. The SCIIC's P/CRCL Policy training program will cover:
- Purposes of the policy.
- Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the center.
- Originating and participating agency responsibilities under the applicable law and policy.
- How to implement the policy in the day-to-day work of a participating agency.
- The potential impact of violations of the policy.
- Mechanisms for reporting violations of the policy.
- How to identify, report, and respond to a suspected or confirmed breach of PII.
- The nature and possible penalties for policy violations, including transfer, dismissal, and criminal liability, if any. Updates to the policy, if any, in response to changes in law and implementation experience.

Appendix A – Terms and Definitions

The following is a list of primary terms and definitions used throughout this P/CRCL Policy.

Access—Data access is being able to get to (usually having permission to use) particular data on a computer. Web access means having a connection to the World Wide Web through an access provider or an online service provider. Data access is usually specified as read-only and read/write access. With regard to the ISE, access refers to the business rules, means, and processes by and through which ISE participants obtain terrorism-related information, to include homeland security information, terrorism information, and law enforcement information acquired in the first instance by another ISE participant.

Access Control—The mechanisms for limiting access to certain information based on a user's identity and membership in various predefined groups. Access control can be mandatory, discretionary, or role-based.

Agency—The SCIIC and all agencies that access, contribute, and share information in the SCIIC's justice information system.

Analysis—The process of converting information from many sources and then developing the most precise and valid inferences possible. The process includes crime analysis and criminal intelligence analysis. The product of analysis is utilized for continued targeting, collection efforts, investigation, or prosecution.

Audit Trail—A generic term for recording (logging) a sequence of activities. 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.

Authentication—The process of validating the credentials of a person, computer process, or device. Authentication requires that the person, process, or device making the request provide a credential that proves it is what or who it says it is. Common forms of credentials are digital certificates, digital signatures, smart cards, biometrics data, and a combination of user names and passwords.

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. See Authentication.

Center—Refers to the SCIIC and all participating state agencies of the SCIIC.

Civil Liberties—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.

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.

Collection—A process in the intelligence cycle which involves the identification and the documentation of actual or planned criminal activity into an investigative or intelligence report.

Computer Security—The protection of information assets through the use of technology, processes, and training.

Confidentiality—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.

Credentials—Information that includes identification and proof of identification that is used to gain access to local and network resources. Examples of credentials are user names, passwords, smart cards, and certificates.

Criminal History Records—Information collected by criminal justice agencies on specific individuals, consisting of official identifiable descriptions and notations of arrests, detentions, warrants, complaints, indictments, information, or other formal criminal charges and any disposition relating to these charges, including acquittal, sentencing, pre- or post- conviction supervision, correctional supervision, and release. Information about victims, complainants, or witnesses who are not otherwise involved with the criminal justice system may be contained in Criminal History Records but will not be used or disclosed.

Criminal Intelligence Information—Information deemed relevant to the identification of and the criminal activity engaged in by an individual who or organization that is reasonably suspected of involvement in criminal activity. Criminal intelligence records are maintained in a criminal intelligence system per 28 CFR Part 23.

Criminal Intelligence System or Intelligence System (as defined by 28 CFR Part 23) —The arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information.

Data—Inert symbols, signs, descriptions, or measures; elements of information.

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—Encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, use, protection, and disclosure of information.

Director of the SC Information and Intelligence Center—Agent appointed by the Chief of SLED to oversee the SCIIC.

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.

Fusion Center—The operations center consisting of analysts, agents, and supervisors; synonymous with SCIIC.

General Information or Data—Information that may include records, documents, or files pertaining to law enforcement operations, such as computer-aided dispatch (CAD) data, incident data, and management information. Information that is maintained in a records management, CAD system, etc., for statistical/retrieval purposes. Information may be either resolved or unresolved. The record is maintained per statute, rule, or policy.

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 (a) relates to a threat of terrorist activity; (b) relates to the ability to prevent, interdict, or disrupt terrorist activity; (c) would improve the identification or investigation of a suspected terrorist or terrorist organization; or (d) would improve the response to a terrorist act.

Identification—A process whereby a real-world entity is recognized and its identity established. Identity is operationalized in the abstract world of information systems as a set of information

about an entity that uniquely differentiates it from other similar entities. The set of information may be as small as a single code, specifically designed as an identifier, or a collection of data, such as a given and family name, date of birth, and address. An organization's identification process consists of the acquisition of the relevant identifying 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, including investigative information; tips and leads data; suspicious activity reports; and criminal intelligence information.

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—The product resulting from the evaluation and interpretation of information, indicating that persons or groups are involved or suspected of involvement in real or suspected criminal activity.

Law—As used by this policy, law includes any local, state, or federal constitution, 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—For purposes of the ISE, 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—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.

Maintenance of Information—Applies to all forms of information storage. This includes electronic systems (for example, databases) and non-electronic storage systems (for example, filing cabinets). To meet access requirements, an organization is not required to create new systems to maintain information or to maintain information beyond a time when it no longer serves an organization's purpose.

Metadata—In its simplest form, metadata is information (data) about information, more specifically information about a particular aspect of the collected information. An item of metadata may describe an individual content item or a collection of content items. Metadata is used to facilitate the understanding, use, and management of information. The metadata required for this will vary based on the type of information and the context of use.

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.

Participating Agency—An organizational entity that is authorized to access or receive and use center information and/or intelligence databases and resources for lawful purposes through its authorized individual users. Those agencies that participate in the operations of the SC Information and Intelligence Center in addition to sharing and collecting information.

Permissions—Authorization to perform operations associated with a specific shared resource, such as a file, directory, or printer. Permissions must be granted by the system administrator to individual user accounts or administrative groups.

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. See also Personally Identifiable Information.

Personally Identifiable Information—One or more pieces of information that, when considered together or in the context of how the information is presented or gathered, are sufficient to specify a unique individual. The pieces of information can be:

- 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 biometrics information, such as fingerprints, DNA, and retinal scans).

- 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, Next Generation Identification [NGI] identifier, or booking or detention system number).
- Descriptions of event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records).
- Descriptions of location(s) or place(s) (including geographic information systems [GIS] locations, electronic bracelet monitoring information, etc.).

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—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 Officer—A SCIIC employee designated by the Captain to ensure compliance with this policy and the ISE privacy guidelines and to serve as the ISE liaison. The privacy officer can be reached at privacyofficer@sled.sc.gov

Privacy Protection—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 includes Personal Information about individuals that is subject to information privacy or other legal protections by law, including the U.S. Constitution and the South Carolina Constitution; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 23; and applicable state law. Protection may also be extended to organizations by center policy and applicable state law.

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 center's information.
- Media organizations.
- 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 center or participating agency.

Public does not include:

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

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.

Reasonable Suspicion/Criminal Predicate—When sufficient facts are established to give a trained law enforcement officer or employee a basis to believe there is a reasonable possibility an individual or organization is involved in a definable criminal activity or enterprise. (28 CFR Part 23)

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—Laws, policies, and procedures that address public agency responsibilities with regard to access/disclosure and correction of information and the handling of complaints from persons regarding protected information about them which is under the center's control and which is exempt from disclosure and not disclosed to the individual to whom the information pertains.

Repudiation—The ability of a user to deny having performed an action that other parties cannot prove otherwise. For example, a user who deleted a file can successfully deny doing so if no mechanism (such as audit files) can contradict that claim.

Requestor—The individual law enforcement officer or agency making a request for information from, or reporting an incident to, the SCIIC.

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.

Right to Privacy—The right to be left alone, in the absence of some reasonable public interest in gathering, retaining, and sharing information about a person's activities. Invasion of the right to privacy can be the basis for a lawsuit for damages against the person or entity violating a person's privacy.

SCIIC Staff—Employees of SLED or other participating agencies assigned to the SCIIC on a full- or part-time basis; includes detailees and contractors supporting SCIIC operations.

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.

South Carolina Information and Intelligence Center or SCIIC—The Intelligence Fusion Center of the South Carolina Law Enforcement Division and participating agencies.

South Carolina Information Exchange (SCIEx) Data Warehouse—The SLED computer system and its data consisting of uniform crime reports submitted by participating SC law enforcement agencies.

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

Storage—In a computer, storage is the place where data is held in an electromagnetic or optical form for access by a computer processor. There are two general usages:
Storage is frequently used to mean the devices and data connected to the computer through input/output operations—that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-computer storage. This is probably the most common meaning in the IT industry.
In a more formal usage, storage has been divided into (1) primary storage, which holds data in memory (sometimes called random access memory, or RAM) and other "built-in" devices such as the processor's L1 cache, and (2) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations.
Primary storage is much faster to access than secondary storage because of the proximity of the storage to the processor or because of the nature of the storage devices. On the other hand, secondary storage can hold much more data than primary storage.
With regard to the ISE, storage (or retention) refers to the storage and safeguarding of terrorism-related information—including 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—Consistent with Section 1016(a)(4) 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.

Terrorism Prevention Act of 2004 (IRTPA) —As amended by the 9/11 Commission Act (August 3, 2007, P.L. 110-53), the ISE facilitates the sharing of terrorism 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 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 intelligence information.
Weapons of Mass Destruction (WMD) information was defined and included in the definition of "terrorism information" by P.L. 110-53.

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 – Applicable Laws

Federal and State laws, regulations and cases:

United States Constitution and Amendments I-XXVII;
The Privacy Act of 1974 (5 U.S.C. 552a);
United States Executive Order 12958 "Classified National Security Information";
United States Department of Justice Criminal Intelligence Systems Operating Policies; 28 CFR Part 23
SC Freedom of Information Act, SC Code Ann. §§30-4-10 et seq.;
SC Code Ann. §39-1-90;
SC Code Ann. §1-11-490, Breach of Security of State Agency Data:
Consumer Protection Code, SC Code Ann. §37-20-110 et seq.;
SC Code Ann. Regulations 73-20 and 73-30;
Intelligence Reform and Terrorism Prevention Act of 2004: 118 STAT. 3666; P.L. 108-458 Section 1016;
6 USC §485;
Snakenberg v. Hartford Cas. Ins., 299 S.C. 164, 383 S.E.2d 2 (Ct. App. 1989)
State v. Houey; 375 SC 106, 651 SE2d 314 (2007)
SLED Policy 9.6;
SCIIC Security Policy

1. South Carolina law:

a. S.C. Constitution art. I, §10 provides that, in regards to searches and seizures, that:

The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures and unreasonable invasions of privacy shall not be violated, and no warrants shall issue but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, the person or thing to be seized, and the information to be obtained.

b. According to the drafters of the 1969 revision of this article, art. I, §10 was recommended for revision to ensure that:

[T]he citizen be given constitutional protection from an unreasonable invasion of privacy by the State. This additional statement ["unreasonable invasions of privacy"] is designed to protect the citizen from improper use of electronic devices, computer data banks, etc.

Final Report of the Committee to Make a Study of the South Carolina Constitution of 1895, p. 15, June, 1969.

c. In Snakenberg v. Hartford Cas. Ins. Co., 299 S.C. 164, 170-71, 383 S.E.2d 2, 5-6 (Ct. App. 1989), the South Carolina Court of Appeals discussed what historically was considered "invasion of privacy," defining two aspects which might have some relevance to a criminal intelligence database:

Wrongful publicizing of private affairs involves a public disclosure of private facts about the plaintiff... The defendant must intentionally disclose facts in which there is no legitimate public interest---there is no right of privacy in public matters. Additionally, the disclosure must be such as would be highly offensive and likely to cause serious mental injury to a person of ordinary sensibilities.
Wrongful intrusion into private affairs, consists of the following element:
(1) Intrusion. An intrusion may consist of watching, spying, prying, besetting, overhearing, or other similar conduct. Whether there is an intrusion is to be decided on the facts of each case.
(2) Into that which is private. The intrusion on the plaintiff must concern those aspects of himself, his home, his family, his personal relationships, and his communications which one normally expects will be free from exposure to the defendant.
(3) Substantial and unreasonable enough to be legally cognizable."

The Court did not discuss art. I, §10, in this case, nor did it discuss a test for determining whether an official inquiry, as opposed to a private act, fails for want of a legitimate public interest or constitutes a wrongful intrusion.

In State v. Houey, 375 SC 106, 651 SE2d 314 (2007) the Court discussed Art. I, Sec. 10 in the context of requiring a defendant to submit to testing for sexually transmitted diseases. In that case, defendant argued that S.C. Code Ann. §16-3-740(B) (providing for testing in such instances) is unconstitutional as violative of Art. I Section 10. The Court stated that:

Although our constitution favors a higher level of privacy protection than the Fourth Amendment..., the testing at issue is not so overly intrusive or unreasonable as to render the statute violative of the South Carolina Constitution." Thus, it appears the Court requires some sort of "overly intrusive or unreasonable" test. The Office of the SC Attorney General Opinions Section has stated that after review of this policy, "designed to collect and circulate in a limited way certain information about individuals for whom a reasonable suspicion of criminal activity exists- would meet this test in that the policy is not 'overly intrusive or unreasonable.' The purpose of such policy- combating terrorist activity- is a legitimate governmental purpose and the means chosen to achieve that purpose is likewise reasonable and not overly intrusive.

No other South Carolina case has been found which discusses under what circumstances collection of information about an individual, as opposed to release of that information, constitutes an unreasonable invasion of personal privacy.

Addressing the first Snakenberg element listed above, wrongful publication, the South Carolina Attorney General has reviewed SLED Regulations 73-20 through 73-30 concerning public release of information in the unified criminal records system and concluded that they comply with United States Department of Justice v. Reporters Committee for Freedom of the Press, 489 U. S. ---, 109 S. Ct. 1468, 103 L. Ed. 2d 774 (1989), and with the South Carolina

Freedom of Information Act, SC Code Ann. §§ 30-4-40, -50, and -70, regarding release of information about an individual to third persons – that is, to persons not engaged in law enforcement or criminal justice. SC AG Op. 90-15, Jan. 24, 1990. The provisions of this policy parallel those of Regulations 73-20 through 73-30.

Addressing the second Snakenberg element, wrongful intrusion, the provisions of Section 2, below, and particularly the prohibitions of section 2.c, articulate the necessity for a legitimate public purpose (a requirement of "reasonable suspicion") to justify collection of information about identified individuals and provide for oversight, restrictions on collection, maintenance and release of that information. It is generally recognized that law enforcement agencies have the authority and obligation to collect information about individuals about whom a reasonable suspicion of criminal activity exists, notwithstanding any desire of the individuals involved to keep it "free from exposure." Homeland security agencies have a similar obligation. Federal regulation 28 CFR Part 23, applicable to federally funded homeland security agencies, explicitly allows collection and protection from unauthorized disclosure of information about actual or potential criminal activity while providing safeguards against profiling and against collection of information about individuals to whom no reasonable suspicion attaches.

S.C. Code Ann. § 1-11-490, Breach of Security of State Agency Data.

(A) An agency of this State owning or licensing computerized data or other data that includes personal identifying information shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of this State whose unencrypted and unredacted personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person when the illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to the resident. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (C), or with measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(B) An agency maintaining computerized data or other data that includes personal identifying information that the agency does not own shall notify the owner or licensee of the information of a breach of the security of the data immediately following discovery, if the personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person.

(C) The notification required by this section may be delayed if a law enforcement agency determines that the notification impedes a criminal investigation. The notification required by this section must be made after the law enforcement agency determines that it no longer compromises the investigation.

(D) For purposes of this section:

(1) "Agency" means any agency, department, board, commission, committee, or institution of higher learning of the State or a political subdivision of it.

(2) "Breach of the security of the system" means unauthorized access to and acquisition of computerized data that was not rendered unusable through encryption, redaction, or other methods that compromise the security, confidentiality, or integrity of personal identifying information maintained by the agency, when illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to the consumer. Good faith acquisition of personal identifying information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system if the personal identifying information is not used or subject to further unauthorized disclosure.

(3) "Personal identifying information" has the same meaning as "personal identifying information" in Section 16-13-510(D).

(E) The notice required by this section may be provided by:

(1) written notice;

(2) electronic notice, if the person's primary method of communication with the individual is by electronic means or is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 USC and Chapter 6, Title 26 of the 1976 Code;

(3) telephonic notice; or

(4) substitute notice, if the agency demonstrates that the cost of providing notice exceeds two hundred fifty thousand dollars or that the affected class of subject persons to be notified exceeds five hundred thousand or the agency has insufficient contact information. Substitute notice consists of:

(a)) e-mail notice when the agency has an e-mail address for the subject persons;

(b) conspicuous posting of the notice on the agency's web site page, if the agency maintains one; or

(c)) notification to major statewide media.

(F) Notwithstanding subsection (E), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal identifying information and is otherwise consistent with the timing requirements of this section is considered to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

(G)) A resident of this State who is injured by a violation of this section, in addition to and cumulative of all other rights and remedies available at law, may:

(1) institute a civil action to recover damages;

(2) seek an injunction to enforce compliance; and

(3) recover attorney's fees and court costs, if successful.

(H) An agency that knowingly and wilfully violates this section is subject to an administrative fine up to one thousand dollars for each resident whose information was accessible by reason of the breach, the amount to be decided by the Department of Consumer Affairs.

(I) If the agency provides notice to more than one thousand persons at one time pursuant to this section, the business shall notify, without unreasonable delay, the Consumer Protection Division of the Department of Consumer Affairs and all consumer reporting agencies that compile and maintain files on a nationwide basis, as defined in 15 USC Section 1681a(p), of the timing, distribution, and content of the notice.