North Carolina Information Sharing and Analysis Center (ISAAC)

1. **Subject: Information Sharing and Analysis Center (ISAAC) Privacy Protection Policy**

2. **Purpose:** To establish written procedures for the protection of the privacy rights, civil rights, and civil liberties of individuals and organizations having information contained within the Information Sharing and Analysis Center (Hereafter referred to as ISAAC).

3. **Oversight:** Daily operations and financial accountability are overseen by the North Carolina State Bureau of Investigation (hereafter denoted as NCSBI). All ISAAC Policies and Procedures are to be reviewed and approved by the NCSBI Assistant Director responsible for the center's operations.

4. **Mission:** ISAAC has a primary responsibility of developing and evaluating information about persons and/or organizations engaged in criminal activity. Specifically, ISAAC's primary mission consists of developing information concerning crimes involving North Carolina Homeland Security, Gangs, and high intensity drug cases. ISAAC acts as a liaison with the NCSBI and other law enforcement agencies engaged in antiterrorism activities, criminal interdiction operations and investigations. ISAAC's principal duties and responsibilities can be categorized as follows: (1) the collection, analysis, and sharing of criminal information; (2) terrorist threat assessment and monitoring; (3) terrorist incident response; (4) development and implementation of special projects, strategies, and initiatives; (5) gang-related activity; and (6) selected organized crime drug cases.

5. **Applicability:** This policy applies to all ISAAC personnel, personnel assigned to ISAAC by partner agencies, personnel providing information technology services to the center, private contractors, partner agencies and stake-holders who use its services, and other authorized users. 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. The Assistant Special Agent in Charge of ISAAC will provide a printed copy of this policy to all center and non-center personnel who provide services, and to participating agencies and individual users, and will require written acknowledgement of receipt of this policy and an agreement of compliance to this policy and the provisions it contains.

a. All ISAAC permanent staff will be required to receive training to recognize behaviors and activities that could be indicative of criminal activity related to terrorism, and familiarize themselves with pertinent databases, as well as the implementation of and adherence to ISAAC policies and procedures, including the Privacy Policy and sanctions for noncompliance with said policies.

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

c. ISAAC's privacy policy training program will cover:

- Purposes of the privacy, civil rights, and civil liberties protection 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 and obligations under applicable law and policy.
- How to implement the policy in the day-to-day work of the user, whether a paper or systems user.
- The impact of improper activities associated with infractions within or through the agency.
- Mechanisms for reporting violations of center privacy protection policies and procedures.
- The nature of and possible penalties for policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.

6. **Policy:** All ISAAC personnel, participating agency personnel, personnel providing information technology services to the center, private contractors, agencies from which center information originates, and other authorized users will comply with all applicable laws and regulations protecting the privacy rights, civil rights, and civil liberties of individuals and organizations including, but not limited to: Public Law 93-579, The Privacy Act of 1974, as amended (5 U.S.C. 552a); Public Law 107-347, Title III of the eGovernment Act of 2002 (The Federal Information Security Management Act of 2002) (44 U.S.C. 101 note); OMB Memorandum No. M-3-22 (OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002); OMB Memorandum No. M-06-15 (Safeguarding Personally Identifiable Information; OMB Memorandum No. M-07-16 (Safeguarding Against and Responding to the Breach of Personally Identifiable Information); Public Law 99-508, The Electronic Communications Privacy Act of 1986; Public Law 95-630, The Right to Financial

Privacy Act of 1978 (12 U.S.C. 3401 note); Public Law 103-322, The Driver's Privacy Protection Act of 1994 (18 U.S.C. 2721 et. seq.); The Privacy Protection Act of 1980 (42 U.S.C. 2000aa et. seq.); Public Law 104-191, The Health Insurance Portability and Accountability Act of 1996 (44 U.S.C. 201 et. seq.); The North Carolina Financial Privacy Act (N.C. Gen. Stat. Chapter 53B); N.C. Gen. Stat. 20-43.1 (limiting the disclosure of personal information in motor vehicle records); N.C. Gen. Stat. 75-65 (requiring notification of security breaches involving personal information); N.C. Gen. Stat. 114-19.50 (The National Crime Prevention and Privacy Compact); N.C. Gen. Stat. 132-1.4 (limiting dissemination of criminal investigations, intelligence information records, Innocence Inquiry Commission records); N.C. Gen. Stat. 132-1.10 (limiting dissemination of social security numbers and other personal identifying information); and The North Carolina Juvenile Code (N.C. Gen. Stat. Chapter 7B) (prohibiting disclosure of juvenile records and other information concerning juveniles). This compliance requirement applies to the collection, use, analysis, retention, destruction, sharing, and disclosure of personal information received and stored within the files and databases at ISAAC. In sharing and disclosing information, ISAAC will also take reasonable measures to ensure the sources of information and methods used to gather information are adequately protected. Information gathered that is determined to be "intelligence information" will be documented and submitted to the Intelligence Section of the NCSBI for entry into the NCSBI Intelligence Management System. This system is operated in compliance with Chapter 28 of the Code of Federal Regulations. Adherence and compliance for the collection, retention and dissemination of said information is maintained pursuant to Chapter 132 of the North Carolina General Statutes and the protections afforded criminal investigative files and criminal intelligence files.

Information-gathering (acquisition) and access and investigative techniques used by ISAAC and information-originating agencies will remain in compliance with and will adhere to applicable laws and guidance, including, but not limited to:

- 28 CFR Part 23, regarding criminal intelligence information.
- The OECD Fair Information Principles (under certain circumstances, there may be exceptions to the Fair Information Principles, based, for example, on authorities paralleling those provided in the federal Privacy Act; state, local, and tribal law; or center policy).
- Criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) *National Criminal Intelligence Sharing Plan* (NCISP).
- Constitutional provisions; Chapter 132 of the North Carolina General Statutes; and administrative rules, as well as regulations and policies that apply to multijurisdictional intelligence and information databases.

ISAAC has adopted internal operating policies that are in compliance with applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to: Public Law 93-579, The Privacy Act of 1974, as amended (5 U.S.C. 552a); Public Law

107-347, Title III of the eGovernment Act of 2002 (The Federal Information Security Management Act of 2002) (44 U.S.C. 101 note); OMB Memorandum No. M-3-22 (OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002); OMB Memorandum No. M-06-15 (Safeguarding Personally Identifiable Information; OMB Memorandum No. M-07-16 (Safeguarding Against and Responding to the Breach of Personally Identifiable Information); Public Law 99-508, The Electronic Communications Privacy Act of 1986; Public Law 95-630, The Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 note); Public Law 103-322, The Driver's Privacy Protection Act of 1994 (18 U.S.C. 2721 et. seq.); The Privacy Protection Act of 1980 (42 U.S.C. 2000aa et. seq.); Public Law 104-191, The Health Insurance Portability and Accountability Act of 1996 (44 U.S.C. 201 et. seq.); The North Carolina Financial Privacy Act (N.C. Gen. Stat. Chapter 53B); N.C. Gen. Stat. 20-43.1 (limiting the disclosure of personal information in motor vehicle records); N.C. Gen. Stat. 75-65 (requiring notification of security breaches involving personal information); N.C. Gen. Stat. 114-19.50 (The National Crime Prevention and Privacy Compact); N.C. Gen. Stat. 132-1.4 (limiting dissemination of criminal investigations, intelligence information records, Innocence Inquiry Commission records); N.C. Gen. Stat. 132-1.10 (limiting dissemination of social security numbers and other personal identifying information); and The North Carolina Juvenile Code (N.C. Gen. Stat. Chapter 7B, prohibiting disclosure of juvenile records and other information concerning juveniles).

7. **Governance and Oversight:** ISAAC has established a multi-disciplinary Governance Board comprised of local, county, state, and federal representation that shall meet quarterly. Discussions shall include, but not be limited to: privacy related issues, tips and leads, community outreach, and policy and procedure for center operations. The Governance Board shall regularly meet at the discretion of the Chairman of the Board to review all policies and procedures of ISAAC and when necessary recommend updating or revising said policies and procedures. The Privacy Policy will be formally reviewed by the Governance Board, Privacy Officer and/or ISAAC staff at least every three years, or sooner if an issue/policy violation is identified that needs immediate attention, to ensure privacy provisions are current and are not in conflict with any other applicable standing policy or state or federal statute.

8. **Compliance:** A trained Privacy Officer will be designated who will receive reports that are submitted through the North Carolina Department of Justice (NCDOJ) Public Information Officer regarding alleged errors and violations of the provisions of this policy; receive and coordinate complaint resolution under the center's redress policy; and serve as the liaison for the Information Sharing Environment (ISE), ensuring that privacy protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy-enhancing technologies. The ISAAC Privacy Officer can be contacted via email through ncisaac@ncdoj.gov. ISAAC, NCSBI leadership, and the Privacy Officer will periodically review and update the provisions protecting privacy, civil rights, and civil liberties contained within this policy and make appropriate changes in response to changes in applicable law, in technology, in the purpose and use of the information systems, and in public expectations.

a. Audits: Financial Audits and Reports will be made to the granting authority and will always adhere to strict North Carolina Department of Justice Financial guidelines. All grants and financial information shall be reviewed and approved by the Chief Fiscal Officer for the North Carolina Department of Justice.

b. Inspections: ISAAC will be subject to inspections and review by the NCSBI. Inspections will occur on a three (3) year rotational basis consistent with other NCSBI Sections and Divisions. These inspections shall comply with the Professional Standards Division of the NCSBI internal off-cycle inspections and shall occur on an unannounced schedule. Internet usage reports shall be run periodically and all employees shall have an internet audit once a year.

c. Division of Criminal Information and Identification Section (CIIS): All CIIS certified operators shall be inspected and reviewed according to the CIIS schedule. Reports shall be conducted on the applicable usage of databases according to NCIC guidelines and the use, access, and dissemination of Criminal History information.

d. CALEA: All units under the direct control and supervision of the NCSBI shall be in compliance with all accreditation standards as stated by the NCSBI Accreditation Section and shall remain in compliance at all times. The NCSBI is an accredited agency recognized by the Association and is noted as a "Flagship" agency.

e. At the discretion of ISAAC leadership, the Privacy Officer and other applicable staff are authorized to review information holdings in order to ensure compliance with the ISAAC privacy policy.

9. **Complaints:** ISAAC personnel will report violations or suspected violations of the privacy policy to the Privacy Officer. The Privacy Officer will assess these complaints and complaints from any other source, including the public and other law enforcement agencies, and if necessary, refer them to the Office of Professional Standards of the NCSBI. All such complaints received regarding violations of the privacy policy will be documented, investigated and retained pursuant to Procedure 24 of the NCSBI Policy and Procedure Manual.

10. **Sanction for Misuse:** In the event any authorized user is found to be in violation of the provisions of this policy or Federal law with regard to collection, use, retention, destruction, sharing, classification, or disclosure of information, the individual will be immediately suspended from access to any information systems and be subject to disciplinary action. If an NCSBI employee is in violation of the provisions of the privacy policy, the individual may be subject to disciplinary action up to and including termination. If the violator is not an NCSBI employee, the individual in violation will be immediately removed from all center operations and denied access to all center databases. Misuse may result in prosecution by federal and/or state authorities for violations of federal and/or state laws including, but not limited to: 18 US 1028 (fraud and related activity in connection with identification documents, authentication features,

and information); 18 USC 1030 (fraud and related activity in connection with computers); N.C. Gen. Stat. 14-454 (accessing computers); N.C. Gen. Stat. 14- 454.1 (accessing government computers); and N.C. Gen. Stat. 14-455 (damaging computers, computer programs, computer systems, computer networks, and resources).

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

11. Procedure:

a. **Seeking & Retaining Information:** In accordance with the Information Sharing Environment Privacy guidelines and the ISAAC Privacy Policy, ISAAC will only seek and/or retain information, except as noted below, on an individual or organization when there is reasonable suspicion that the individual or organization has committed a criminal offense, or is planning criminal conduct or activity (including terrorism) that presents a threat to any individual, the community, or the nation. Furthermore, the information sought and/or retained must be information that is relevant to the criminal conduct or activity. Additionally, ISAAC will only seek information concerning individuals and organizations in response to requests for support from field operating elements engaged in an ongoing law enforcement investigation or event, and/or non-law enforcement agencies/entities for health and public safety purposes. This information includes, but is not limited to: criminal history, public records as defined by N.C. Gen. Stat. Chapter 132, open source information, suspicious activity reports, etc. The information retained and generated by ISAAC will not exceed Sensitive but Unclassified (SBU) information and will be categorized and labeled as *Law Enforcement Sensitive (LES)* when applicable. All other information is deemed Unclassified (U), which may or may not be for ISAAC personnel official use only. If originally unclassified information is later determined to be of investigative interest or sensitive in nature, this information may be subsequently categorized as LES.

ISAAC will only seek and/or retain protected information that is legally permissible for the agency to seek and/or retain under the laws, regulations, and policies applicable to ISAAC per Article 4 Part 1 of N.C. Gen. Stat. Ch. 114.

Individuals assigned to ISAAC will ensure that retained protected information has been lawfully obtained.

ISAAC applies labels to center-originated information (or ensures that the originating agency has applied labels) to indicate to the accessing authorized user that:

- The information is "protected information," to include "personal data" on any individual (see section O. Definitions) and, to the extent expressly provided in this policy, includes organizational entities.

- The information is subject to laws restricting access, use, or disclosure, including but not limited to: The North Carolina Financial Privacy Act (N.C. Gen. Stat. Chapter 53B); N.C. Gen. Stat. 20-43.1 (limiting the disclosure of personal information in motor vehicle records); The North Carolina Juvenile Code (N.C. Gen. Stat. Chapter 7B, prohibiting disclosure of juvenile records other information concerning juveniles); Article 7 of the State Personnel Act (N.C. Gen. Stat. Chapter 126, requiring adherence to privacy of State employee personnel records); and N.C. Gen. Stat. 132-1.1 through 132-1.12 (defining certain information as confidential and/or not public record; and limiting access, disclosure or dissemination as to certain information).

ISAAC will not seek or retain, and information-originating agencies will agree not to submit, information about an individual or organization solely on the basis of their lawful activities; religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their race, ethnicity, citizenship, place of origin, age, disability, gender or sexual orientation.

Information gathering and investigative techniques used by ISAAC will be, and those used by originating agencies should be, the least intrusive means necessary in the particular circumstances to gather information it is authorized to seek and/or retain.

External agencies that access ISAAC'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. External agencies must also comply with the Information Sharing and Analysis Center (ISAAC) Privacy Protection Policy.

Nothing in this document shall be construed to limit the ability of ISAAC to initiate, without a specific request, short-term research or information gathering regarding events or activities being publically reported in the media which may impact health and public safety in North Carolina.

ISAAC will not directly or indirectly receive, seek, accept, or retain information from:

- An individual who, or nongovernmental entity that may or may not receive a fee or benefit for providing the information, except as expressly authorized by law or center policy.

- An individual who, or information provider that is legally prohibited from obtaining or disclosing the information.

ISAAC will receive, seek, accept, or retain information from individuals who have received compensation through Crimestoppers or other such entity.

b. **Process:** As information is received at ISAAC, it is initially documented by the Administrative Assistant, ISAAC investigators, and/or the analysts. Information is immediately evaluated by the ISAAC supervisor, who filters, prioritizes, and

disseminates the information. When appropriate, the ISAAC supervisor assigns ISAAC personnel to conduct follow-up investigation and analysis. After review by the ISAAC supervisor and/or designee, the "raw" information is forwarded to the analyst/LEO, who reviews it within the context of his or her own particular areas of interest and responsibility. The analyst/LEO may subsequently recommend certain actions to ISAAC supervisors and/or his or her own agency/organization to manage the consequences of an activity. Information collected by ISAAC is initially logged into the ISAAC Tips and Leads Activity Log. Access to the aforementioned log is restricted to ISAAC personnel. If the information is deemed to have reached the level of reasonable suspicion of criminal activity by ISAAC supervisors, ISAAC agents and/or analysts are assigned to conduct follow-up investigations and analysis regarding the raw information will make every reasonable effort to better determine its credibility, accuracy, and relevancy, and to gather additional relevant information. Criminal information, to include transcripts of source documentation that meets the criteria for investigative support, is entered into the ISAAC data warehouse (ETeams), where it is assigned a tracking number and logged for case progression. Case progression and inputs from internal ISAAC staff are tagged in a manner that identifies the information provider for records and case tracking purposes.

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

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

ISAAC 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.

Investigations that arise from information are documented in the case management system as possible criminal activity investigations. Information that is determined to be intelligence information will be documented and submitted to the Intelligence Section (this NCSBI component is external to ISAAC) for entry into the NCSBI

Intelligence Management System. This system is operated in compliance with Chapter 28, Part 23 of the federal Code of Regulations and requirements set forth therein, and its data is available for query and analysis by NCSBI Criminal Intelligence Analysts. Information deemed investigative will be accessible by approved law enforcement agencies/personnel in North Carolina.

ISAAC personnel will, upon receipt of information, 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 has assigned categories to the information) to reflect the assessment, such as:

- Whether the information consists of tips and leads data, suspicious activity reports, criminal history, intelligence information, case records, conditions of supervision, case progress, or other information category.
- 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).

ISAAC will keep a record of the source of all information sought and collected by the center.

Information that is received by ISAAC that the reviewer determines is "reasonably indicative" of criminal or terrorist activity that has occurred, is occurring, or may occur, but falls below the "reasonable suspicion" threshold, hereafter referred to as a Suspicious Activity Reporting (SAR), shall be processed in a separate manner. *Information that is reasonably indicative that criminal or terrorist activity has, is or may occur, but falls short of "reasonable suspicion" may be information that an individual is observed measuring or photographing a significant public landmark on a regular or repeated basis without an obvious innocent purpose*. It will then be vetted for criminal information by being provided to an appropriate/responsible agency with access to an approved SAR database such as the FBI's E-Guardian system. The SAR process consists of human review and vetting to ensure that information is both legally gathered and, where applicable, determined to have a potential terrorism nexus. ISAAC personnel will be trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism. This process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved in activities associated with terrorism will be documented and shared through the ISE. These safeguards are intended to ensure that information that could violate civil rights and civil liberties will not be intentionally or inadvertently gathered, documented, processed and shared. The

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

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

Information provided into the E-Guardian system is properly labeled, enabling ISE-authorized users to identify Personal Identifiable Information (PII) or other protected information in the reporting in order to identify information that may need to be minimized if further dissemination is necessary. SARs are processed in the standard reporting format in which other tips and leads are processed. The ISAAC's SAR process is subject to manual review by the Privacy Officer and other staff as deemed necessary by ISAAC leadership to ensure information is legally gathered and disseminated.

i. Full-time authorized ISAAC staff will be permitted access to the data warehouse. All other external partners will have access to the information contained in the data warehouse at the discretion of the ISAAC staff, which determines that the requestor has a "need to know" and a "right to know" the information.

ISAAC personnel are required to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of SAR information. Center personnel will:

- Prior to allowing access to or dissemination of the information, ensure that attempts to validate or refute the information have taken place, and that the information has been assessed for sensitivity and confidence by subjecting it to an evaluation or screening process to determine its credibility and value, and categorize the information as unsubstantiated or uncorroborated if attempts to validate or determine the reliability of the information have been unsuccessful.

- Store the information using the same storage method used for data that rises to the level of reasonable suspicion and that includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information.

- 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.

- Regularly provide access to or disseminate the information in response to an interagency inquiry for law enforcement, homeland security, 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.

- Retain information for a period of no more than five (5) years in order to determine its credibility and value or assign a "disposition" label so that a subsequently authorized user knows the status and purpose for the retention and will retain the information for no more than five (5) years unless it is validated for an additional retention period or a determination is made that audit/administrative requirements prevent deletion (in which case the information will not be searchable).

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

- Incorporate the SAR process into existing processes and systems used to manage other crime-related information and criminal intelligence, thus leveraging existing policies and protocols utilized to protect the information, as well as information privacy, civil rights, and civil liberties.

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

c. **Information Quality Assurance:** As previously stated, ISAAC will make every reasonable effort to ensure that information collected and/or retained is derived from dependable and trustworthy sources, accurate, current, and complete, including the relevant context in which it was sought or received. At the time of retention, the information will be properly labeled with respect to the information's sensitivity as well as assessed reliability and quality. The labeling of retained information will be reevaluated by ISAAC or the originating agency when new information is gathered that has an impact on confidence (source reliability and content validity) in previously retained information.

ISAAC will conduct periodic data quality reviews of information it originates, and make every reasonable effort to ensure that the information will be corrected, deleted from the system, or not used when (i) the center identifies information that is erroneous, misleading, obsolete, or otherwise unreliable; (ii) the center did not have

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

If information arises that suggests errors or deficiencies in ISAAC information holdings, the Privacy Officer, in conjunction with the ISAAC staff, will make every reasonable effort to investigate said errors and/or deficiencies and initiate action to correct, confirm or otherwise authenticate the information. If investigation results in confirming the deficiencies, all holdings subject to the allegations will be updated to reflect the correct data. If investigation results in a correction to the data which would make retention of the information in violation of the ISAAC Privacy Policy, or state or federal statue, the information will be appropriately purged from retention systems in accordance with guidelines set forth by 28 CFR, Part 23. ISAAC will provide notice of this correction, in writing or via electronic communication, to agencies that generated and/or received the information in question.

i. ISAAC will contract only with commercial database entities that provide an assurance that their methods for gathering Personally Identifiable Information comply with applicable local, state, tribal, territorial, and federal laws, statutes, and regulations, and that these methods are not based on misleading information-gathering practices. (For example, a commercial database should not gather information in contravention with 18 U.S.C. § 2510, more commonly known as Title III.)

d. **Limitations on Access to and Disclosure of Information:** ISAAC will appropriately limit access to information, or the disclosure of information, concerning individuals and organizations it has obtained to those personnel who are authorized to receive and use such information. Access will be granted and/or disclosure permitted *only* to authorized individuals, who *must* adhere to the policy and procedures stated herein as well as all applicable federal and state laws.

Credentialed, role-based access criteria will be used by ISAAC, 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.

Only limited information access is granted and/or disclosure permitted in order to ensure that ISAAC protects an individual's right of privacy, civil rights and civil liberties. As previously stated, this information will be labeled to indicate its sensitivity in order to convey to the user the protected status of the information.

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

- Protect confidential sources and police undercover techniques and methods.
- Not interfere with or compromise pending criminal investigations.
- Protect an individual's right of privacy or his or her civil rights and civil liberties.
- Provide legally required protections based on the individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, resident of a domestic abuse shelter or participant in the Address Confidentiality Program pursuant to N.C. Gen. Stat. Ch15C .

e. **Collection, Collation, and Analysis of Information:** Information sought or received by ISAAC, or from other sources, will *only* be used to provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of engaging in criminal or terrorist activities, and to further crime prevention (including terrorism), enforcement, force deployment, or prosecution objectives and priorities established by the Secretary of the North Carolina Department of Crime Control and Public Safety and pursuant to guidelines established by the Attorney General of North Carolina.

Information acquired or received by ISAAC will be analyzed only by qualified individuals that have undergone a background screening from their respective parent agencies and have received appropriate training. All information discussed in paragraph11a is subject to collation and analysis according to priorities and needs in order to further crime prevention, public safety, and priorities established by the center.

Records about an individual or organization from two or more sources will not be merged by ISAAC unless there is sufficient information to reasonably conclude the information is about the same individual or group. The set of identifiers sufficient to allow merging will consist of all available attributes that can contribute to a higher accuracy of match. If sufficient information is not available about suspected matching records they will be prohibited from being merged until such a threshold is reached.

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

f. **Sharing Of Information With Other Partners:** Access to information gathered or retained by ISAAC will *only* be provided to persons within ISAAC or to criminal justice, public safety, or regulatory agencies with authorized access. Even those agencies or entities with authorized access *must* use the information *only* for legitimate law enforcement, public protection, prosecution, or other criminal justice purposes, and then *only* in the performance of official duties in accordance with applicable laws and procedures. In accordance with the Standard Operating Procedures of the NCSBI, an audit trail will be kept of access to ISAAC information or the dissemination of ISAAC information to individuals. Agencies external to the ISAAC may not further disseminate information accessed or disseminated from the center without approval from ISAAC staff or other originator of the information.

    i. Information that is provided via broad distribution to agencies not specifically involved with a subject investigation may receive LES information that has had Personally Identifiable Information (PII) redacted from the product. (For example, persons of interest in a report may be labeled as "subject" or "individual" etc.) Redacted information may be provided to a partner agency upon request and at the discretion of the ISAAC staff. Permission for partner agencies to forward ISAAC generated information to third parties may be granted upon request and at the discretion of the ISAAC staff.

g. **Sharing Of Information With Those Responsible For Public Protection, Safety, Or Health:** Information gathered or retained by ISAAC *may* be disseminated to non-criminal justice public or private entities *only* for public protection, critical infrastructure protection, safety, or public health purposes, and *only* in the performance of official duties in accordance with applicable law and procedures ensuring that PII is minimized to the greatest extent necessary to accomplish the mission. Role-based access to information will be determined on a case-by-case basis and will be distributed via written or electronic means. 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.

h. **Sharing Of Information For Specific Purposes:** Information gathered or collected and records retained by ISAAC may be accessed or disseminated ***for specific purposes*** upon request by persons authorized by law to have such access and only for those uses and purposes specified in the law. An audit trail sufficient to allow the identification of each individual who requested, accessed, or received information retained by the center; the nature of the information requested, accessed, or received; and the specific purpose will be kept for a minimum of five (5) years by the center.

i. **Disclosure of Information to the Public:** Information gathered and retained by ISAAC will be disclosed to an individual member of the public in accordance with N.C. Gen. Stat. Chapter 132.

Information gathered or collected and records retained by ISAAC 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 to further the center's mission and is not exempt from disclosure by law. Such information may be disclosed only in accordance with the law and procedures applicable to the center for this type of information. An audit trail sufficient to allow the identification of 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. ISAAC will not confirm the existence or nonexistence of any information to any person or organization that would not be eligible to receive the information itself pursuant to N.C.G.S. §132-1.4 concerning criminal investigative files and criminal intelligence files. In general, information classified as "for official use only" and above is not and will not be released to the public without request, review and consent from ISAAC Leadership staff.

Information gathered or collected and records retained by ISAAC ***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.

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

- Records required to be kept confidential by law are exempted from disclosure requirements under the following, but are not limited to: Public Law 93-579, The Privacy Act of 1974, as amended (5 U.S.C. 552a); Public Law 107-347, Title III of the eGovernment Act of 2002 (The Federal Information Security Management Act of 2002) (44 U.S.C. 101 note); OMB Memorandum No. M-3-22 (OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002); OMB Memorandum No. M-06-15 (Safeguarding Personally Identifiable Information; OMB Memorandum No. M-07-16 (Safeguarding Against and Responding to the Breach of Personally Identifiable Information); Public Law 99-508, The Electronic Communications Privacy Act of 1986; Public Law 95-630, The Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 note); Public Law 103-322, The Driver's Privacy Protection Act of 1994 (18 U.S.C. 2721 et. seq.); The Privacy Protection Act of 1980 (42 U.S.C. 2000aa et. seq.); Public Law 104-191, The Health Insurance Portability and Accountability Act of 1996 (44 U.S.C. 201 et. seq.); The North Carolina Financial Privacy Act (N.C. Gen. Stat. Chapter 53B); N.C. Gen. Stat. 20-43.1 (limiting the disclosure of personal information in motor vehicle records); N.C. Gen. Stat. 75-65 (requiring notification of security breaches involving personal information); N.C. Gen. Stat. 132-1.4 (limiting dissemination of criminal

investigations, intelligence information records, Innocence Inquiry Commission records); N.C. Gen. Stat. 132-1.10 (limiting dissemination of social security numbers and other personal identifying information); and The North Carolina Juvenile Code (N.C. Gen. Stat. Chapter 7B) (prohibiting disclosure of juvenile records and other information concerning juveniles).

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

- Investigatory records of law enforcement agencies that are exempted from disclosure requirements under N.C.G.S. §132-1.4 concerning criminal investigative files and criminal intelligence files. However, certain law enforcement records must be made available for inspection and copying under N.C. Gen. Stat. 132-1.4(c).

- A record or part of a record the public disclosure of which would have a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack is exempted from disclosure requirements under N.C. Gen. Stat. 132-1.7. This includes a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism under N.C. Gen. Stat. 132-1.7 or an act of agricultural terrorism under N.C. Gen. Stat. 132-1.7, vulnerability assessments, risk planning documents, needs assessments, and threat assessments.

- Protected federal, state, local, or tribal records, which may include records originated and controlled by another agency that cannot be shared without permission pursuant to, but are not limited to, Public Law 93-579, The Privacy Act of 1974, as amended (5 U.S.C. 552a); Public Law 107-347, Title III of the eGovernment Act of 2002 (The Federal Information Security Management Act of 2002) (44 U.S.C. 101 note); OMB Memorandum No. M-3-22 (OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002); OMB Memorandum No. M-06-15 (Safeguarding Personally Identifiable Information; OMB Memorandum No. M-07-16 (Safeguarding Against and Responding to the Breach of Personally Identifiable Information); Public Law 99-508, The Electronic Communications Privacy Act of 1986; Public Law 95-630, The Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 note); Public Law 103-322, The Driver's Privacy Protection Act of 1994 (18 U.S.C. 2721 et. seq.); The Privacy Protection Act of 1980 (42 U.S.C. 2000aa et. seq.); Public Law 104-191, The Health Insurance Portability and Accountability Act of 1996 (44 U.S.C. 201 et. seq.); The North Carolina Financial Privacy Act (N.C. Gen. Stat. Chapter 53B); N.C. Gen. Stat. 20-43.1 (limiting the disclosure of personal information in motor vehicle records); N.C. Gen. Stat. 75-65 (requiring notification of security breaches involving personal information); N.C. Gen. Stat. 132-1.4 (limiting dissemination of criminal investigations, intelligence information records, Innocence Inquiry Commission records); N.C. Gen. Stat. 132-1.10 (limiting dissemination of

social security numbers and other personal identifying information); and The North Carolina Juvenile Code (N.C. Gen. Stat. Chapter 7B, prohibiting disclosure of juvenile records and other information concerning juveniles).

- A violation of an authorized nondisclosure agreement will be handled pursuant to the terms and conditions of the agreement itself.

j. **Redress:** In the event that an individual or entity feels that information collected or maintained by ISAAC, about the individual or entity, was collected or maintained in violation of Chapter 28 of the Code of Federal Regulations Part 23 or N.C.G.S 114-12, the individual or entity shall first be directed to file a formal complaint with the State Bureau of Investigation Headquarters via phone at 919.662.4500. If an individual has a complaint with regard to the accuracy or completeness of terrorism-related protected information that:

(1) Is exempt from disclosure,
(2) Has been or may be shared through the ISE,
  (a) Is held by ISAAC and
  (b) Allegedly has resulted in demonstrable harm to the complainant,

The center will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Upon receiving a complaint, the center shall forward the complaint to the NCSBI Assistant Director, ISAAC Director and Privacy Officer for action. The Privacy Officer shall acknowledge the receipt of the complaint to the complaining party and assure the complaining party that **if** information is held by ISAAC related to the complaining party it will be reviewed to insure that it conforms to federal regulation; and if it does not conform, that it will be purged. The Privacy Officer will next determine **if** ISAAC does in fact maintain information about the individual or entity. If ISAAC does in fact maintain information about the individual or entity, the Privacy Officer should first determine whether the information rises to the level of reasonable suspicion that the individual or entity has committed a criminal offense, or is planning criminal conduct or activity (including terrorism) that presents a threat to any individual, the community, or the nation. Second, the Privacy Officer should make every effort to ensure that information collected and/or retained is derived from dependable and trustworthy sources; and is accurate, current, and complete, including the relevant context in which it was sought or received. Third, the Privacy Officer should consult with the ISAAC Staff and Legal Counsel to determine whether the information should be corrected or purged from retention systems in accordance with guidelines set forth in 28 CFR, Part 23. If the information did not originate with the center, the Privacy Officer will notify the originating agency in writing or electronically within 10 days and, upon request, assist such agency to correct any identified data/record deficiencies, purge the information, or verify that the record is accurate. All information held by the center that is the subject of a complaint will be reviewed within 30 days and confirmed; or corrected/purged if determined to be inaccurate or incomplete, to include incorrectly merged information, or to be out of date. If there is no resolution within 30 days, the

center will not share the information until such time as the complaint has been resolved. A record of requests for redress and the actions taken as a result should be maintained by the Privacy Officer.

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

k. **Disclosure:** Any request for disclosure of information by an individual or entity should be directed to the North Carolina Department of Justice Public Information Officer (PIO), who can be contacted via e-mail at ntalley@ncdoj.gov or via telephone at 919-716-6413. The PIO will forward the request to the Privacy Officer, who shall acknowledge the receipt of the request to the individual or entity and assure them that if information is held by ISAAC related to the request; it will be reviewed to determine whether there is information which may be disseminated pursuant to the request. Next, the Privacy Officer will determine whether information related to the request is held by ISAAC. If such information exists, the Privacy Officer should consult with the ISAAC Supervisor and Legal Counsel to determine whether the information may be disseminated pursuant to North Carolina General Statute §132-1.4 or federal regulation. Information which can be disseminated pursuant to North Carolina General Statute §132-1.4 or federal regulation shall be disseminated by the Privacy Officer accompanied by a written response. Upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity and subject to the conditions specified 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 ISAAC. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information. The center's response to the request for information will be made within a reasonable time and in a form that is readily intelligible to the individual.

   The Privacy Officer shall maintain a record of requests for disclosure of information and any response to such a request. Any other dissemination to an individual or entity that cannot be disseminated pursuant to North Carolina General Statute §132-1.4 or federal regulation shall require the order of a court of competent jurisdiction. The existence, content, and source of the information will not be made available by ISAAC to an individual 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 in a criminal intelligence information system subject to 28 CFR Part 23 [see 28 CFR § 23.20(e)].

- The information is subject to North Carolina General Statute §132-1.4.
- The information source does not reside with the center.
- The center did not originate and does not have a right to disclose the information.
- Other ***authorized*** basis for denial.

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 disclosure **by the center** or referral **of the requestor** to the source agency was neither required nor appropriate under applicable law.

l. **Complaints and Corrections:** In the event that an individual or entity feels that information collected or maintained by ISAAC about the individual or entity is inaccurate or incomplete, the individual or entity shall first be directed to file a formal complaint with the State Bureau of Investigation Headquarters via phone at 919.662.4500, outlining their concerns in detail. Upon receiving said complaint, the SBI shall forward the complaint to the Privacy Officer for action. The Privacy Officer shall acknowledge the receipt of the complaint to the complaining party and assure the complaining party that if information is held by ISAAC related to the complaining party it will be reviewed, in light of their complaint, to ensure that it conforms with federal regulation; and if it does not, that it will be purged. The Privacy Officer will next determine if ISAAC does in fact maintain information about the individual or entity. If ISAAC does in fact maintain information about the individual or entity, the Privacy Officer should first determine whether the information rises to the level of reasonable suspicion that the individual or entity has committed a criminal offense, or is planning criminal conduct or activity (including terrorism) that presents a threat to any individual, the community, or the nation. Second, the Privacy Officer should make every effort to ensure that information collected and/or retained is derived from dependable and trustworthy sources; and is accurate, current, and complete, including the relevant context in which it was sought or received. If the information is deemed to be erroneous, to include incorrectly merged information, or to be out of date, the information will be corrected or purged from the ISAAC database. If the information is owned by a participating agency, ISAAC personnel will inform the agency electronically of the complaint, and provide any needed assistance in investigating and correcting or removing the information prior to any further dissemination. A record will be kept of all complaints and request for corrections and the resulting action taken, if any.

m. **Appeals:** The individual who has requested disclosure or to whom information has been disclosed will be given reasons if disclosure or requests for corrections are denied by ISAAC or the originating agency. The individual will also be informed of the procedure for appeal when the center or originating agency has cited an

exemption for the type of information requested or has declined to correct challenged information to the satisfaction of the individual to whom the information relates.

n. **Information Retention and Destruction:** All applicable retained ISAAC information will be reviewed for record retention in accordance with 28 CFR Part 23, to include purging of applicable data that has not been updated within five (5) years from last update. When information has no further legitimate value or meets the criteria for removal according to ISAAC's retention and destruction policy, it will be purged, destroyed, deleted, or returned to the submitting source if required by the governing document(s) with the approval of ISAAC staff. The ISAAC data warehouse properly documents information that has been identified for destruction, and identifies information and notifies staff that it has reached the five (5) year retention limitations mentioned above. No approval will be required from the originating agency before information held by ISAAC is destroyed or returned in accordance with this policy or as otherwise agreed upon with the originating agency in a participation or membership agreement. A record of information to be reviewed for retention will be maintained by ISAAC, and for appropriate system(s), notice will be given to the submitter at least 30 days prior to the required review and validation/purge date. Notification of proposed destruction or return of records may or may not be provided to the originating agency by ISAAC, depending on the relevance of the information and any agreement with the originating agency. If information is determined to be relevant or under an agreement with the originating agency, notice will be given at least 30 days prior to the required review and validation/purge date.

o. **Information System Transparency:** ISAAC will be open with the public in regard to information and intelligence collection practices. This privacy policy establishing protections of privacy rights, civil rights, and civil liberties will be provided to the public for review, made available to the public upon request, kept on file with the Director of ISAAC or his/her designee, and posted on the center's public-facing Web site at http://secure.nccrimecontrol.org/hsb/pages/isaac.aspx. Formal inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s) maintained or accessed by the center can be processed through the State Bureau of Investigation Headquarters via phone at 919.662.4500.

p. **Information Security:** While the ISAAC Director has overall responsibility for the physical security of the center and is the trained and Designated Security Officer, the FBI and DHS are responsible for their respective designated spaces. The ISAAC Director will delegate Security Officer Responsibilities to the ISAAC Deputy Director. Additionally, the North Carolina Department of Justice has provided an Information Technology Officer (ITO) on a part-time basis. This ITO will ensure that ISAAC-IT operating systems are functioning properly and all prescribed information security guidelines prescribed by North Carolina Department of Justice are followed. Furthermore, this individual will see that all ISAAC-IT related software is implemented onto the ISAAC's computer database systems and the proper use of

these computer database systems is being followed by ISAAC staff. The ITO will be a qualified individual who has received proper training in this discipline.

i. All center personnel will receive security training which covers physical, information and operational security principles. Access to ISAAC information will be granted only to center personnel whose positions and job duties require such access; who have successfully completed a background check and appropriate security clearance, if applicable; and who have been selected, approved, and trained accordingly.

ii. Technical safeguards and procedures of the ISAAC facility and the secured storage of information contained within are described in further detail in the NC-ISAAC Standard Operating Procedures for Protecting and Safeguarding of Open Storage of Classified National Security Information dated May 2010. Access to ISAAC facilities and operating environments are controlled by building security to include cardkey systems. Access to the ISAAC file room is limited to ISAAC personnel only. No other personnel are allowed access to the file room without specific authorization from an ISAAC supervisor or designee. Where applicable, procedures for safeguarding classified information are laid out in the NC-ISAAC Standard Operating Procedures for Protecting and Safeguarding of Open Storage of Classified National Security Information dated May 2010.

iii. Access to ISAAC electronic systems will be provided in a manner that ensures individual sign-on and password information is made available in order to provide the ability of assigning role-based access when applicable as well as auditing information that has been accessed by internal personnel.

iv. Queries made to ISAAC's data applications will be logged into the data system identifying the user who initiates the query.

v. ISAAC will utilize watch logs to maintain audit trails of requested and disseminated information.

vi. ISAAC will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with system requirements and with the provisions of this policy and applicable law. This will include logging access to these systems and periodic auditing of these systems, so as to not establish a pattern of the audits. These audits will be mandated at least annually and a record of the audits will be maintained by the Privacy Officer.

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

viii. In the event of a data breach of any sort, the ISAAC will execute procedures and guidelines laid out in the North Carolina Department of Justice-Information Technology Division Incident Management Plan as directed by the General Assembly amended statute GS 147-33.82.

ix. The ISAAC director will ensure the center operates in a secure facility protected from external intrusion, and will establish procedures and practices that use software, information technology tools, and physical security measures to protect information from unauthorized access, modification, theft or sabotage. The center will utilize secure internal and external safeguards against network intrusions. Access to the center's databases from outside the facility will be allowed only over secure networks. The center will store information in a manner that cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions.

q. **Accountability for Activities:** Primary responsibility for the operation of the ISAAC information system, enforcement of this policy, and sanctions for noncompliance (see section 10. Sanction for Misuse) are assigned to the Director of ISAAC and/or his or her designee. At a minimum, the Director or his or her designee will:

i. Require individuals authorized to access ISAAC's systems to agree in writing to comply with the provisions of this policy.

ii. Periodically and randomly conduct audits of the information receipt, analysis, dissemination, and storage processes addressed in this policy memorandum. The audit will be conducted in such a manner so as to protect the confidentiality, sensitivity, and privacy of the information.

r. Definitions:

i. **Criminal Information** –Information historical, strategic, and/or tactical that is pertinent to:
- The identification of persons, groups, or organizations that commit criminal acts, or are engaged in activities in support of, or in preparation of, the commission of criminal acts;
- The investigation of specific criminal acts by local, state, or federal law enforcement agencies, and the identification, arrest, and prosecution of the perpetrators of such acts or incidents;
- The prediction and subsequent prevention of criminal acts through collection, integration, investigation, evaluation, and sharing of such information;
- Additionally, *Criminal Information* involves circumstances that establish sufficient facts to give a trained law-enforcement or criminal investigative agency, officer, investigator, or employee a basis to believe that there is reasonable possibility that an individual or organization is involved in criminal activities.

ii. **Data Warehouse** – The ISAAC data warehouse is the records management system used to store information processed through the center.

iii. **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 investigation or meet another law enforcement requirement.

iv. **Personal Data -** Personal data refers to any information that relates to an identifiable individual (or data subject). See also Personally Identifiable Information.

v. **Personally Identifiable Information** - Information that can be used to uniquely identify, contact, or locate a single person; or can be used with other sources to uniquely identify a single individual. (Examples of PII are full names, social security number, driver's license number, etc). The term "identifying information" as defined in N.C. Gen. Stat. 14-113.20(b) includes the following: (1) Social security or employer taxpayer identification numbers; (2) Drivers license, State identification card, or passport numbers; (3) Checking account numbers; (4) Savings account numbers; (5) Credit card numbers; (6) Debit card numbers; (7) Personal Identification (PIN) Code as defined in G.S. 14-113.8(6); (8) Electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names; (9) Digital signatures; (10) Any other numbers or information that can be used to access a person's financial resources; (11) Biometric data; (12) Fingerprints; (13) Passwords; (14) Parent's legal surname prior to marriage.

vi. Protected Information – Protected information includes Personal Data about individuals that is subject to information privacy or other legal protections by law, including the U.S. Constitution and the North Carolina constitution; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 23; applicable state and tribal constitutions; and applicable state, local, and tribal laws and ordinances. Protection may also be extended to organizations by center policy or state, local, or tribal law.

vii. **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.

viii. **Reasonable Suspicion of Criminal Activity** – A set of circumstances that establishes sufficient facts to give a trained law-enforcement or criminal investigative agency, officer, investigator, or employee a basis to believe

that there is reasonable possibility that an individual or organization is involved in criminal activities.

ix. **Suspicious Activity Reporting (SAR) –** Official documentation of observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity. SAR information offers a standardized means for 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 designated to support interagency calls for service.

x. **Tips and Leads Information -** Uncorroborated report or information generated from inside or outside the agency that alleges or indicates some form of possible criminal activity.