Southern Nevada Counter-Terrorism Center

Privacy, Civil Liberties, and Civil Rights Protection Policy

Table of Contents

Southern Nevada Counter-Terrorism Center
Privacy, Civil Liberties and Civil Rights Protection Policy[1]

A. Purpose Statement

The purpose of the Southern Nevada Counter-Terrorism Center (SNCTC) Privacy, Civil Rights, and Civil Liberties Protection Policy (hereafter "Privacy and CR/CL Policy") is to promote the Southern Nevada Counter-Terrorism Center (hereafter "SNCTC" or "submitting agency"), source agency, and user agency (hereafter collectively referred to as "participating agencies" or "participants") conduct that complies with applicable federal, state, local, and tribal laws, regulations, and policies and assists participants in:

- Ensuring 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.

The SNCTC project was initiated in response to the increased need for timely information sharing and exchange of crime-related information among members of the law enforcement community. One component of the SNCTC focuses on the development and exchange of criminal intelligence. This component focuses on the intelligence process where information is collected, integrated, evaluated, analyzed and disseminated.

The SNCTC's intelligence products and services will be made available to law enforcement agencies, criminal justice entities, and other designated organizations. All agencies participating in the SNCTC will be subject to a Memorandum of Understanding and will be required to adhere to all SNCTC policies and security requirements. The purpose of this privacy policy is to ensure safeguards and sanctions are in place to protect personal identifying data as information and intelligence are developed and exchanged.

This Privacy Policy embraces the eight Privacy Design Principles developed by the Organization of Economic Cooperation and Development's Fair Information Practices and shall be used to guide the policy wherever applicable. The eight Privacy Design Principles are:

[1] The Southern Nevada Counter-Terrorism Center gratefully acknowledges the contributions of the Indiana Intelligence Fusion Center; the Institute for Intergovernmental Research (IIR); the United States Department of Justice, Bureau of Justice Assistance (BJA); the Organization of Economic Cooperation and Fair Information Practices; the Association of Law Enforcement Intelligence Units (LEIU); the Criminal Intelligence Coordinating Council / Global Intelligence Working Group.

- *Purpose Specification—Define agency purposes for information to help ensure agency uses of information are appropriate.*
- *Collection Limitation—Limit the collection of personal information to that required for the purposes intended.*
- *Data Quality—Ensure data accuracy.*
- *Use Limitation—Ensure appropriate limits on agency use of personal information.*
- *Security Safeguards—Maintain effective security over personal information.*
- *Openness —Promote a general policy of openness about agency practices and policies regarding personal information.*
- *Individual Participation—Allow individual's reasonable access and opportunity to correct errors in their personal information held by the agency.*
- *Accountability—Identify, train, and hold agency personnel accountable for adhering to agency information quality and privacy policies.*

B. Policy Applicability and Legal Compliance

All participating SNCTC personnel (including participating agency personnel and personnel providing information technology services to the SNCTC), private contractors, and other authorized participants will comply with applicable provisions of the SNCTC's Privacy and CR/CL Policy concerning personal information, including those referenced in Appendix A and the following:

- SAR information the source agency collects and the SNCTC receives.
- The ISE-SAR information identified, submitted to the shared space, and accessed by or disclosed to SNCTC personnel.
- Criminal intelligence as defined in 28 CFR Part 23 that the SNCTC collects, stores, maintains and shares.
- Criminal history information as defined in Nevada Revised Statutes (NRS) 179A.070.
- Investigative reports and investigative working files as provided in NRS 179A.070.
- Nevada Public Records Law, NRS 239 et seq.
- Homeland Security - Confidential and Restricted Documents, NRS 239C.

The SNCTC will provide a printed copy of its Privacy and CR/CL Policy to all SNCTC personnel, non-agency personnel who provide services to the SNCTC, and to each source agency and SNCTC 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.

All SNCTC 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 and state, local, and federal privacy, civil rights, civil liberties, and legal requirements applicable to the SNCTC and/or other participating agencies

The SNCTC has adopted internal operating policies that are in compliance with applicable law protecting privacy, civil rights, and civil liberties, including, but not limited to the United States Constitution, the Nevada Constitution, and all Federal, state and local laws, rules and ordinances (See Appendix A, State and Federal Laws Relevant to Seeking, Retaining and Disseminating Justice Information).

C. Governance and Oversight

1. The Southern Nevada Counter-Terrorism Center Director will have primary responsibility for operating the SNCTC, all information and intelligence files; ISE-SAR information system operations, and coordinating personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing or disclosure of SAR and ISE-SAR information; and enforcing the provisions of this policy.

   The SNCTC is guided by a designated Board of Governors, that liaises with the community to ensure that privacy and civil rights are protected as provided in this policy and by the SNCTC's information gathering and collection, retention, and dissemination processes and procedures.

2. The SNCTC's Board of Governors is guided by a trained Privacy Officer who is contracted or assigned by the SNCTC Director to assist in enforcing the provisions of this policy and who, in addition to other responsibilities, will receive reports regarding alleged errors and violations of the provisions of this policy. The Privacy Officer can be contacted at the following address: Privacy@snctc.org.

D. Definitions

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.

Acquisition—The means by which an ISE participant obtains information through the exercise of its authorities, for example, through human intelligence collection or from a foreign partner. For the purposes of this definition, acquisition does not refer either to the obtaining of

information widely available to other ISE participants through, for example, news reports or to the obtaining of information shared with them by another ISE participant who originally acquired the information.

Agency—The Southern Nevada Counter-Terrorism Center (SNCTC) and all agencies that access, contribute, and share information in the SNCTC's justice information system.

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 (usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

Center—Center refers to the Southern Nevada Counter-Terrorism Center (SNCTC).

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" refers to governments' 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.

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

Data—Elements of information.

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

Fusion Center—A collaborative effort of two or more agencies that provide resources, expertise, and information to a designated government agency or agency component with the goal of maximizing its ability to detect, prevent, investigate, and respond to criminal and terrorist activity.

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.

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

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

ISE—Information Sharing Environment. A trusted partnership among all levels of government, the private sector, and foreign partners to detect, prevent, preempt and mitigate the effects of terrorism against territory, people, and interests of the United States of America. This partnership enables the trusted, secure, and appropriate exchange of terrorism information, in the first instance, across the five federal communities; to and from the state, local and tribal governments, foreign allies, and the private sector; and at all levels of security classifications. (Baseline Capabilities 3/10/08 p. 57)

ISE-SAR—A suspicious activity report that has been determined, pursuant to a two-part process, to have a potential terrorism nexus. ISE-SAR business rules will serve as a unifying process to support the reporting, tracking, processing, storage, and retrieval of terrorism-related suspicious activity reports across the ISE.

ISE-SAR Information Exchange Package Documentation (IEPD) A schema that facilitates the posting and sharing of ISE-SAR information. The ISE-SAR IEPD is used to represent ISE information in two different data formats:

(1) The **Detailed format** includes information contained in all data elements set forth in Section IV of the ISE-SAR FS ("ISE-SAR Exchange Data Model"), including fields denoted as privacy fields.

(2) The **Summary format** excludes certain privacy fields as identified in the ISE-SAR FS. The ISE-SAR FS identifies the minimum privacy fields that must be excluded. Each ISE participant may exclude additional privacy fields from its Summary ISE-SARs, in accordance with applicable legal requirements.

Law—As used by this policy, law includes any local, state, or federal statute, ordinance, regulation, executive order, policy, or court rule, decision, or order as construed by appropriate local, state, or federal officials or agencies.

Law Enforcement Information—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—See Audit Trail. Logs are a necessary part of an adequate security system because they are needed to ensure that data is properly tracked and that only authorized individuals can access the system and the data.

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.

Participating Agencies—Participating agencies, for purposes of the EE Initiative, include source **[the agency or entity that originates SAR (and, when authorized, ISE-SAR) information]**, submitting (the agency or entity posting ISE-SAR information to the shared space), and user (an agency or entity authorized by the submitting agency or other authorized agency or entity to access ISE-SAR information, including information in the shared space(s), and which may include analytical or operational component(s) of the submitting or authorizing agency or entity) agencies, in support of their responsibility to collect, document, process, access, or use SAR and ISE-SAR information.

Personal Data—Personal data refers to any information that relates to an identifiable individual. See also Personally Identifiable Information.

Personally Identifiable Information—Personally identifiable information is 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, marks, 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, Automated Integrated Fingerprint Identification System [AFIS] 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.).

Privacy—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 right 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 Fields—Data fields in ISE-SAR IEPDs that contain personal information.

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

Privacy Protection—A process of maximizing the protection of privacy, civil rights, and civil liberties when collecting and sharing information in the process of protecting public safety and public health.

Protected Information—Protected information is information about any individual that is subject to information privacy or other legal protections under the Constitution and laws of the United States and the State of Nevada. These protections are derived from applicable state and local laws and ordinances. It also includes organizations as expressly provided in this policy.

Public—Public includes:

- Any person and any for-profit or nonprofit entity, organization, or association.
- Any governmental entity for which there is no existing specific law authorizing access to the agency's/center's information.
- Media organizations.
- Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the agency.

Public does not include:

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

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.

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.

Role-Based Access—A type of access that uses roles to determine rights and privileges. A role is a symbolic category of users that share the same security privilege.

Security—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.

Shared Space—A networked data and information repository which is under the control of submitting agencies and which provides terrorism-related information, applications, and services to other ISE participants.

Sharing—The act of one ISE participant disseminating or giving homeland security information, terrorism information, or law enforcement information to another ISE participant.

Source Agency—The agency or 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:

1. 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 meaning is probably more common in the Information Technology industry than the second meaning.

2. 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, to include homeland security information, terrorism information, and law enforcement information relating to terrorism or the security of our homeland by both the originator of the information and any recipient of the information.

Submitting Agency—The agency or entity providing ISE-SAR information to the shared space.

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-Related Information—In accordance with the IRTPA, as recently amended by the 9/11 Commission Act enacted on August 3, 2007 (P.L. 110-53), the ISE facilitates the sharing of terrorism and homeland security information, as defined in the 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 IRTPA, as well as the following categories of information to the extent that they do not otherwise constitute "terrorism information": (1) homeland security information as defined in Section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. § 482(f)(1)) and (2) law enforcement information relating to terrorism or the security of our homeland). Such additional information includes intelligence information.

Weapons of Mass Destruction (WMD) information as a fourth (third statutory) category of ISE information is not called for in P.L. 110-53. Rather, it amends the definition of terrorism information to include WMD information and then defines that term. WMD information probably should not technically be cited or referenced as a fourth category of information in the ISE.

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 SNCTC's information and intelligence databases and resources for lawful purposes.

User Agency—The agency or entity authorized by the submitting agency or other authorized agency or entity to access ISE-SAR information in the shared space(s), which may include analytical or operational component(s) of the submitting or authorizing agency or entity.

E. Information

1. The SNCTC has established a mechanism to create access to existing data sources from participating entities to share data with the goal of identifying, developing, and analyzing information and intelligence related to terrorist activity and other crimes for investigative leads. This capability will facilitate integration and exchange of information between the participating agencies.

2. The SNCTC will seek or retain information that:
   a. Is based on a criminal predicate or possible threat to public safety; or
   b. Is based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal (including terrorist) conduct or activity; or
   c. Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime; or
   d. is useful in a crime analysis or in the administration of criminal justice and public safety (including topical searches); and he 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.

3. The SNCTC 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, however this information will be kept separate and segregated from criminal intelligence files and criminal history information.

4. The SNCTC 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 non-criminal organization or lawful event; or their race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation.

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

- The information is subject to Federal and Nevada state laws restricting access, use, or disclosure, including, but not limited to, 18 USC 2721, et seq., NRS 179A, 239 and 239C.210; and
- The information is protected information, as defined by the SNCTC, to include personal data on any individual (see definitions of "protected information" and "personal data" in Section D of this policy), and, to the extent expressly provided in this policy, includes organizational entities.

6. The SNCTC 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 will assign categories to the information) to reflect the assessment, such as:

   a. Whether the information consists of tips and leads data, suspicious activity reports, criminal history or intelligence information, case records, conditions of supervision, or case progress, etc.;
   b. The nature of the source as it affects veracity (for example, anonymous tip, trained interviewer or investigator, public record, private sector);
   c. The reliability of the source (for example, reliable, usually reliable, unreliable, unknown); and
   d. The validity of the content (for example, confirmed, probable, doubtful, cannot be judged).

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

   a. Protect confidential sources and police undercover techniques and methods;
   b. Not interfere with or compromise pending criminal investigations;
   c. Protect an individual's right of privacy, civil rights, and civil liberties; and
   d. Provide legally required protection based on the individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.

8. The classification of existing information will be re-evaluated whenever:

   a. New information is added that has an impact on access limitations or the sensitivity of disclosure if the information; or
   b. 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.

9. SNCTC personnel are required to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of tips and leads and suspicious activity report (SAR) information. SNCTC personnel will:

a. Prior to allowing access to or dissemination of the information, ensure that attempts to validate or refute the information have taken place and that the information has been assessed for sensitivity and confidence by subjecting it to an evaluation or screening process to determine its credibility and value and categorize the information as unsubstantiated or uncorroborated if attempts to validate or determine the reliability of the information have been unsuccessful. The SNCTC will use a standard reporting format and data collection codes for SAR information.
b. Store the information using the same storage method used for data that rises to the level of reasonable suspicion and includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information.
c. Allow access to or disseminate the information using the same (or a more restrictive) access or dissemination standard that is used for data that rises to the level of reasonable suspicion (for example, "need-to-know" and "right-to know" access or dissemination).
d. Regularly provide access to or disseminate the information in response to an interagency inquiry for law enforcement, homeland security, or public safety and analytical purposes or provide an assessment of the information to any agency, entity, individual, or the public when credible information indicates potential imminent danger to life or property.
e. Retain information long enough to investigate 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. This retention period will not exceed one (1) year unless it can be demonstrated that reasonable suspicion exists to believe that the actor(s) are engaged in, or about to engage in, criminal activity, including terrorism.
f. Adhere to and follow the agency's/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.

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

11. The SNCTC will identify and review information that is originated by the SNCTC prior to sharing that information in the ISE. Further, the SNCTC 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.

12. The SNCTC requires certain basic descriptive information 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 should include:

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

13. The SNCTC 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.

14. The SNCTC will keep a record of the source of all information retained by the agency.

F. Acquiring and Receiving Information

1. Information gathering (acquisition and access) and investigative techniques used by the SNCTC and information-originating agencies are in compliance with and will adhere to applicable regulations and guidelines, including, but not limited to:

    a. 28 CFR Part 23 regarding criminal intelligence information
    b. Organization for Economic Co-operation and Development's (OECD) *Fair Information Practices* (under certain circumstances, there may be exceptions to the *Fair Information Practices*, based, for example, on authorities paralleling those provided in the federal Privacy Act; state, local, and tribal laws; or agency/center policy);
    c. Applicable criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) *National Criminal Intelligence Sharing Plan* (NCISP)
    d. Applicable constitutional provisions, NRS 179A and 239, and any applicable administrative rules, as well as any other regulations that apply to multijurisdictional intelligence databases.

2. The SNCTC'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 SNCTC personnel will be trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism.

3. The SNCTC's SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved in behaviors that have been determined to be consistent with criminal activities associated with terrorism will be documented and shared through the ISE. These safeguards are intended to ensure that information that could violate civil rights and civil liberties (e.g., race, culture, religion, or political associations) will not be intentionally or inadvertently gathered, documented, processed, and shared.

4. Information gathering and investigative techniques used by the SNCTC will (and for originating agencies should) be the least intrusive means necessary in the particular circumstances to gather information it is authorized to seek or retain.

5. External agencies that access and share information with the SNCTC are governed by the laws and rules governing those individual agencies, as well as by applicable federal and state laws.

6. The SNCTC 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 collection practices.

7. The SNCTC will not directly or indirectly receive, seek, accept, or retain information from:

    a. An individual or nongovernmental entity who may or may not receive a fee or benefit for providing the information, except as expressly authorized by law or center policy; or
    b. An individual or information provider that is legally prohibited from obtaining or disclosing the information.

G. Information Quality Assurance

1. The SNCTC 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. At the time of retention in the system, the information will be labeled regarding its level of quality (accurate, complete, current, verifiable, and reliable).

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

4. The labeling of retained information will be reevaluated when new information is gathered that has an impact on the confidence (validity and reliability) in previously retained information.

5. The SNCTC will conduct periodic data quality reviews of information it originates and will make every reasonable effort to ensure that information will be corrected, deleted from the system, or not used when the agency/center learns that the information is erroneous, misleading, obsolete, or otherwise unreliable; the source of the information did not have authority to gather the information or to provide the information to the agency; or the source used prohibited means to gather the information, except when the source did not act as an agent to a bona fide law enforcement officer.

6. Originating agencies external to the SNCTC are responsible for the quality and accuracy of the data accessed by or provided to the SNCTC. The SNCTC will advise the appropriate contact person in the originating agency, in writing, if its data is alleged, suspected or found to be inaccurate, incomplete, out of date, or unverifiable.

7. The SNCTC will use written or documented electronic notification to inform recipient agencies when information previously provided to the recipient agency is deleted or changed by the SNCTC. For example, when the information is determined to be erroneous, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the rights of the individual may be affected.

H. Analysis

1. Information acquired or received by the SNCTC or accessed from other sources will be analyzed only by qualified individuals who have successfully completed a background check and appropriate security clearance, if applicable, and have been selected, approved, and trained accordingly.

2. Information subject to collation and analysis is information as defined and identified in the section, “Information.”

3. Information acquired or received by the SNCTC or accessed from other sources is analyzed according to priorities and needs and will be analyzed only to:

a. Further crime prevention (including terrorism), enforcement, force deployment, or prosecution objectives and priorities established by the SNCTC, and
b. Provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal (including terrorist) activities.

I. Merging and Combining Records

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

2. 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 adequately established that the information relates to the same individual or organization.

J. Sharing and Disclosure

1. Credentialed, role-based access criteria will be used, as appropriate, to control:

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

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

3. Access to or disclosure of records retained by the SNCTC will be provided only to persons within other governmental agencies or private sector entities 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. An audit trail will be kept of access by or dissemination of information to such persons.

4. Agencies external to the SNCTC may not disseminate SNCTC information received from SNCTC without approval from the originator of the information. This requirement does not apply to information that was already provided to or disclosed to, or independently acquired by, the SNCTC without restrictions from its originating source and disseminated to agencies external to the SNCTC by the SNCTC. The external agencies may be required to obtain approval from the SNCTC to disseminate the information received from the SNCTC as needed.

5. Records retained by the SNCTC may be accessed or disseminated to those responsible for public protection, safety, or public health only for public protection, safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures. An audit trail will be kept of access by or dissemination of information to such persons.

6. Information gathered and records retained by the SNCTC may be accessed or disseminated for specific purposes upon request by persons authorized by law to have such access and only for those users and purposes specified in the law. An audit trail will be kept for a minimum of three (3) years of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.

7. Information gathered and records retained by the SNCTC 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 SNCTC mission and is not exempt from disclosure by law. Such information may be disclosed only in accordance with the laws of the State of Nevada for this type of information. An audit trail will be kept of all requests and of what information is disclosed to a member of the public.

8. Information gathered and records retained by the SNCTC will not be:

    a. Sold, published, exchanged, or disclosed for commercial purposes;
    b. Disclosed or published without prior notice to the originating agency that such information is subject to re-disclosure or publication, unless disclosure is agreed to as part of the normal operations of the agency; or
    c. Disseminated to persons not authorized to access or use the information.

9. There are several categories of records that will ordinarily not be provided to the public under Chapter 179A and/or Chapter 239 of the Nevada Revised Statutes:

    a. Records required to be kept confidential by law are exempted from disclosure requirements under NRS 179A, 239 or NRS 239C, subsection 210.

b. Investigatory records of law enforcement agencies are exempted from disclosure requirements under NRS 179A.070. However, certain law enforcement records must be made available for inspection and copying under NRS 239.
c. Criminal Intelligence Information: NRS 179A.070 declares that criminal intelligence information is not considered to be criminal history information, and is not subject to release and disclosure as defined in NRS 179.100, unless access to the records is specifically required by a state or federal statute or is ordered by a court under the rules of discovery. Participating agencies providing data remain the owners of the data contributed and, as such, are responsible for granting access when required by applicable federal or state law or court order.
d. A record or part of a record the public disclosure of which would have a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack is exempted from disclosure requirements under NRS 239C.210. This includes a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism or an act of agricultural terrorism, vulnerability assessments, risk planning documents, needs assessments, and threat assessments.
e. Protected federal, state, local, or tribal records, which may include records originated and controlled by another agency that cannot be shared without permission, unless they are required to be disclosed, including information that meets the definition of "classified information" as that term is defined in the National Security Act, Public Law 235 Section 606 and in accordance with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010.
f. Records in violation of an authorized nondisclosure agreement.

10. Subject only to the requirement of SNCTC to comply with the 179A.100 or NRS 239 or other applicable law, the SNCTC shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.

11. SNCTC participating agencies providing data remain the owners of the data contributed to the SNCTC. The SNCTC may be required by statute, regulation, or mutual agreement, to use or disseminate the data in a particular manner. Members of the public can access individually identifiable information on themselves from the SNCTC, as permissible by law, by making a request under the Nevada Access to Public Records Act or other law permitting access, or by making a request to the originating agency. Persons wishing to access data pertaining to themselves should communicate directly with the agency or entity that is the source of the data.

12. Citizen inquiries to the SNCTC about personal data are the responsibility of the SNCTC Director. The SNCTC Director will notify the agency who is the owner or originator of the data of the request. The agency shall designate in

writing to the SNCTC which of those records, if any, the agency considers confidential information or otherwise excepted from disclosure under exceptions to NRS 179A or 239. The SNCTC shall promptly review the basis for the agency's claims, including claims of confidentiality under federal laws, and shall not disclose the records subject to the agency's claims if the SNCTC concurs with the agency's claims. If the SNCTC determines that its obligations under NRS 179A or 239 requires such disclosure, the SNCTC shall promptly notify the agency of such determination and will not make such disclosure if the agency obtains, prior to the expiration of the applicable timeframe to respond to such request, either an opinion from the Clark County District Attorney's Office or the Nevada Office of the Attorney General that such disclosure is not required, or a protective order or other relief from any court of competent jurisdiction preventing such disclosure.

13. Participating agencies agree that they will notify owners of the information of requests related to individually identifiable information.

14. Upon receipt of a request for one or more documents under NRS 179A or 239, SNCTC personnel will immediately contact an attorney Las Vegas Metropolitan Police Department Office of General Council or the Clark County District Attorney's Office for assistance in responding to the request. The requestor will be afforded a prompt response, with consideration to the breadth and complexity of the request.

K. Disclosure and Correction/Redress

1. Upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity and subject to the conditions specified in K.1 (2), 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 SNCTC. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information. The SNCTC'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. A record will be kept of all requests and of what information is disclosed to an individual.

2. Pursuant to the SNCTC's lawful discretion, the existence, content, and source of the information will not be made available to an individual, unless required by Nevada statute of other law, when:

    a. Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution;
    b. Disclosure would endanger the health or safety of an individual, organization, or community;
    c. The information is in a criminal intelligence system;

d. The information is classified under federal law.
e. The information source does not reside with the SNCTC; or
f. The SNCTC did not originate or does not have a right to disclose the information.

The SNCTC Director will notify the agency who is the owner or originator of the data of the request.

L. Complaints and Corrections

1. If an individual has complaints or objections to the accuracy or completeness of information about him or her ***originating with the agency***, including information that may be shared through the ISE, the SNCTC's privacy official 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.

2. If an individual has complaints or objections to the accuracy or completeness of information about him or her that ***originates with another agency***, including information that is shared through the ISE, the SNCTC's privacy official or designee will notify the originating agency of the complaint or request for correction and coordinate with the originating agency to assist the individual with complaint and corrections procedures. A record will be kept of all such complaints and requests for corrections and the resulting action taken, if any.

3. If an individual has a complaint or objection to the accuracy or completeness of terrorism-related information that has been or may be shared through the ISE that:

   a. is held by the SNCTC;
   b. allegedly resulted in harm to the complainant; and
   c. is exempt from disclosure, the SNCTC will inform the individual of the procedure for submitting (if needed) and resolving complaints or objections. Complaints should be directed to the SNCTC Privacy Officer at the following e-mail address: Privacy@snctc.org. The SNCTC will acknowledge the complaint and state that it will be reviewed, but will not confirm the existence of the information that is exempt from disclosure, as permitted by law. If the information did not originate with the SNCTC, SNCTC will notify the originating agency in writing or electronically within 10 days and, upon request, assist such agency to correct or purge any identified data/record deficiencies, subject to applicable records retention procedures, or to verify that the record is accurate. Any personal information originating with the SNCTC that is the subject of the complaint will be reviewed within 30 days and confirmed or corrected/purged if determined to be inaccurate or incomplete, include incorrectly merged information, or to be out of date. If there is no resolution within 30 days, the SNCTC will not share the information until such time as the complaint has been resolved. A record will

be kept of all complaints and requests for corrections and the resulting action, if any.

4. An individual to whom information has been disclosed will be given reasons if requests for correction(s) are denied by the SNCTC or originating agency, including ISE participating agencies, and be informed of the existing procedure for appeal. To delineate protected information shared through the ISE from other data, the SNCTC maintains records of agencies sharing terrorism-related information and audit logs and employs system mechanisms to identify the originating agency when the information is shared.

    a. An appeal panel shall meet with the individual to resolve issues related to the correction or removal of information from the shared databases of the SNCTC. The panel shall be comprised of the SNCTC Director; the Records Manager/Director of the agency contributing this information to the SNCTC; and a representative from the Clark County District Attorney's Office. All decisions resulting from this meeting will be final.
    b. The panel shall meet with the complaining person with 30 days of the receipt of the challenge or complaint by the Privacy Officer.

M. Security Safeguards

1. The SNCTC Director is designated and trained to serve as the SNCTC's Security Program Administrator.

2. The SNCTC will operate in a secure facility protecting the facility from external intrusion. The SNCTC will utilize secure internal and external safeguards against network intrusions. Access to SNCTC databases from outside the facility will be allowed only over secure networks.

3. The SNCTC will secure tips, leads, and SAR information in a separate repository system that is the same as or similar to the system that secures data rising to the level of reasonable suspicion.

4. Queries made to the SNCTC data applications will be logged into the data system identifying the user initiating the query.

5. The SNCTC will utilize watch logs to maintain audit trails of requested and disseminated information.

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

7. The SNCTC will store information in a manner such that it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions.

8. Access to SNCTC information will be granted only to SNCTC 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.

9. The SNCTC will notify an individual about whom personal information was or is reasonably believed to have been breached or obtained by an unauthorized person and access to which threatens physical, reputational, or financial harm to the person. The notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or any measures necessary to determine the scope of the release of information and, if necessary, to reasonably restore the integrity of any information system affected by this release.

N. Information Retention and Destruction

1. All applicable information will be reviewed for record retention (validation or purge) at least every five (5) years, as provided by 28 CFR Part 23, or for a longer or shorter period specified by regulation or manual adopted pursuant to NRS 239 and Nevada Administrative Code 239. In cases of information other than criminal intelligence, the information will be reviewed every five (5) years to determine whether a law, rule, regulation or court order mandates the retention or purging of the information.

2. When information has no further value or meets the criteria for removal according to the SNCTC's retention and destruction policy or according to applicable law, it will be purged, destroyed, and deleted or returned to the submitting source.

3. The SNCTC will delete information or return it to the source unless it is validated, as specified in 28 CFR Part 23.

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

5. A record of information to be reviewed for retention will be maintained by the SNCTC and, for appropriate systems, notice will be given to the submitter at least 30 days prior to the required review and validation/purge date.

O. Accountability and Enforcement

1. Information System Transparency

a. The SNCTC will be open with the public in regard to information and intelligence collection practices. The SNCTC privacy policy will be provided

to the public for review, will be made available upon request, and posted on the SNCTC Web site at www.snctc.org. Requests for a copy of the privacy policy can made to the SNCTC Privacy Officer at the following e-mail address: Privacy@snctc.org.

b. The SNCTC 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). The Privacy Officer can be contacted by e-mail at the following address: Privacy@snctc.org.

2. Accountability

a. The audit log of queries made to the SNCTC will identify the user initiating the query.

b. The SNCTC will maintain an audit trail of accessed, requested, or disseminated information. An audit trail will be kept for a minimum of three (3) years of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.

c. The SNCTC will provide a copy of this policy to all agency/center and non-SNCTC personnel who provide services and will require written acknowledgement of receipt of this policy and agreement of compliance to this policy and the provisions it contains.

d. The SNCTC will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with their systems, in provisions of this policy and applicable law. This will include logging access of 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 quarterly, and a record of the audits will be maintained by the Deputy Director for Intelligence and Analysis of the agency.

e. The SNCTC's personnel or other authorized users shall report violations or suspected violations of agency/center policies relating to protected information to the SNCTC Privacy Officer.

f. The SNCTC will annually conduct an audit and inspection of the information contained in its criminal intelligence system. The audit will be conducted by a designated independent panel. This independent panel has the option of conducting a random audit, without announcement, at any time and without prior notice to the SNCTC. This audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the agency's/center's criminal intelligence system.

g. The SNCTC Board of Governors, guided by the appointed and trained Privacy Officer, will review and update the provisions protecting privacy,

civil rights, and civil liberties contained within this policy annually and will make appropriate changes in response to changes in applicable law, technology, the purpose and use of the information systems, and public expectations.

h. The SNCTC will notify an individual about whom sensitive personally identifiable information was or is reasonably believed to have been breached or obtained by an unauthorized person and access to which threatens physical, reputational, or financial harm to the person. The notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or any measures necessary to determine the scope of the release of information and, if necessary, to reasonably restore the integrity of any information system affected by this release.

3. Enforcement

1. If an authorized user is found to be in noncompliance with the provisions of this policy regarding the collection, use, retention, destruction, sharing, classification, or disclosure of information, the Executive Director of the SNCTC will:

   a. Suspend or discontinue access to information by the user;

   b. Terminate the assignment of the user to the SNCTC, as permitted by the SNCTC Memorandum of Understanding;

   c. Apply administrative actions or sanctions as provided by rules and regulations or as provided in employing agency personnel policies;

   d. Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

2. The SNCTC reserves the right to restrict the qualifications and number of personnel having access to SNCTC information and to suspend or withhold service to any personnel violating the privacy policy. The SNCTC reserves the right to deny access to any participating agency user who fails to comply with the applicable restrictions and limitations of the SNCTC Privacy Policy.

P. Training

1. The SNCTC will require the following individuals to participate in training programs regarding implementation of and adherence to the privacy, civil rights, and civil liberties policy:

a. All assigned personnel of the SNCTC
b. Personnel providing information technology services to the SNCTC
c. Staff in other public agencies or private contractors providing services to the agency,
d. Users who are not employed by the SNCTC or a contractor.

2. The SNCTC will provide special training to personnel authorized to share protected information through the ISE regarding the SNCTC requirements and policies for collection, use, and disclosure of protected information.

3. The SNCTC privacy policy training program will cover:

a. Purposes of the privacy, civil rights, and civil liberties protection policy;
b. Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the SNCTC;
c. Originating and participating agency responsibilities and obligations under applicable law and policy;
d. How to implement the policy in the day-to-day work of the user, whether a paper or systems user;
e. The impact of improper activities associated with infractions within or through the agency;
f. Mechanisms for reporting violations of agency/center privacy-protection policies; and
g. The nature and possible penalties for policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.

Appendix A

State and Federal Laws Relevant to Seeking, Retaining, and Disseminating Justice Information

State of Nevada Laws:

Constitution of the State of Nevada

Nevada Revised Statues (NRS) including, but not limited to:

- NRS-179A, Records of Criminal History and Information Related to Public Safety;
- NRS-179A.070, Investigative reports and investigative working files;
- NRS-239, Public Records;
- NRS-239C, Homeland Security;
- NRS-241, Public Meetings;
- NRS-480, Administration of Laws Relating to Public Safety, Section 460(3) Duties of the Chief of Division; and
- NRS-603A, Security of Personal Information in Electronic Systems.

Federal Laws:

Brady Handgun Violence Prevention Act, 18 U.S.C. §§ 921, 922, 924, and 925A, United States Code, Title 18, Part I, Chapter 44, §§ 921, 922, 924, and 925A

Computer Matching and Privacy Act of 1988, 5 U.S.C. § 552a(a), United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a(a); see also Office of Management and Budget, Memorandum M-01-05, "Guidance on Interagency Sharing of Personal Data–Protecting Personal Privacy," December 20, 2000

Confidentiality of Identifiable Research and Statistical Information, 28 CFR Part 22, Code of Federal Regulations, Title 28, Chapter I, Part 22

Crime Identification Technology, 42 U.S.C. § 14601, United States Code, Title 42, Chapter 140, Subchapter I, § 14601

Criminal History Records Exchanged for Noncriminal Justice Purposes, 42 U.S.C. § 14611, United States Code, Title 42, Chapter 140, Subchapter II, § 14611

Criminal Intelligence Systems Operating Policies, 28 CFR Part 23, Code of Federal Regulations, Title 28, Chapter 1, Part 23

Criminal Justice Information Systems, 28 CFR Part 20, Code of Federal Regulations, Title 28, Chapter 1, Part 20

Disposal of Consumer Report Information and Records, 16 CFR Part 682, Code of Federal Regulations, Title 16, Chapter I, Part 682

Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2522, 2701–2709, United States Code, Title 18, Part I, Chapter 119, §§ 2510–2522, 2701–2709, and 3121–3125, Public Law 99-508

Fair Credit Reporting Act, 15 U.S.C. § 1681, United States Code, Title 15, Chapter 41, Subchapter III, § 1681

Federal Civil Rights laws, 42 U.S.C. § 1983, United States Code, Title 42, Chapter 21, Subchapter I, § 1983

Federal Records Act, 44 U.S.C. § 3301, United States Code, Title 44, Chapter 33, § 3301

Freedom of Information Act (FOIA), 5 U.S.C. § 552, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552

HIPAA, Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 201, United States Code, Title 42, Chapter 6A, Subchapter I, § 201; Public Law 104-191

HIPAA, Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164; Code of Federal Regulations, Title 45, Parts 160 and 164

Indian Civil Rights Act of 1968, 25 U.S.C. § 1301, United States Code, Title 25, Chapter 15, Subchapter I, § 1301

Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Section 1016, as amended by the 9/11 Commission Act

National Child Protection Act of 1993, Public Law 103-209 (December 20, 1993), 107 Stat. 2490

National Crime Prevention and Privacy Compact, 42 U.S.C. § 14616, United States Code, Title 42, Chapter 140, Subchapter II, § 14616

Privacy Act of 1974, 5 U.S.C. § 552a, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a

Privacy of Consumer Financial Information, 16 CFR Part 313, Code of Federal Regulations, Title 16, Chapter I, Part 313

Protection of Human Subjects, 28 CFR Part 46, Code of Federal Regulations, Title 28, Chapter 1, Volume 2, Part 46

Safeguarding Customer Information, 16 CFR Part 314, Code of Federal Regulations, Title 16, Chapter I, Part 314

Sarbanes-Oxley Act of 2002, 15 U.S.C., Chapter 98, § 7201, United States Code, Title 15, Chapter 98, § 7201

U.S. Constitution, First, Fourth, and Sixth Amendments

USA PATRIOT Act, Public Law 107-56 (October 26, 2001), 115 Stat. 272

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

December 7, 2010

Lieutenant Tom Monahan
Southern Nevada Counter-Terrorism Center
6767 Spencer Street
Las Vegas, NV 89119

Dear Lieutenant Monahan:

The Intelligence Reform and Terrorism Prevention Act of 2004, as amended by the Implementing Recommendations of the 9/11 Commission Act of 2007, established an information sharing environment for the sharing of terrorism-related information while protecting the privacy, civil rights, and civil liberties of individuals. The *Guidelines to Ensure that Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment* ("ISE Privacy Guidelines") require relevant entities, including fusion centers, to have a written privacy protection policy in place that is "at least as comprehensive" as the ISE Privacy Guidelines.

In my capacity as a co-chair of the Privacy and Civil Liberties Sub-Interagency Policy Committee, I have reviewed the Southern Nevada Counter-Terrorism Center privacy policy and recognize it to be "at least as comprehensive" as the ISE Privacy Guidelines. Fusion center privacy policies should be renewed and updated as necessary based on any future changes to the ISE Privacy Guidelines.

Completion of this written privacy policy is an important first step in the implementation of a strong privacy protection framework, to include training of fusion center personnel in privacy and civil liberties protections. In fostering trust among the public and your partners, I urge you to make this policy available to the public through a variety of different channels, to include electronic means. Centers must supply a copy of this privacy policy upon request, but I also recommend you post it on any public facing website your center maintains and be prepared to discuss it as you liaise with your local communities.

Finally, I strongly recommend that your center begin preparing a Privacy Impact Assessment (PIA) or updating an existing PIA, if applicable. A PIA is a vital tool used to evaluate possible privacy risks and to mitigate identified risks to the privacy, civil rights, and civil liberties of individuals. The Global Justice Information Sharing Initiative's *Guide to Conducting Privacy Impact Assessments for State, Local, and Tribal Information Sharing Initiatives* can be found at http://www.it.ojp.gov/default.aspx?area=privacy&page=1295 and is a useful resource in PIA development.

Should you have any questions with regard to privacy issues, please feel free to contact the DHS Privacy Office on behalf of the Privacy and Civil Liberties Sub-IPC at 703-235-0780.

Sincerely,

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

cc: Alexander W. Joel, ODNI CLPO
Nancy C. Libin, DOJ CP&CLO
Margo Schlanger, DHS Officer for Civil Rights and Civil Liberties
Mikeal Johnston, Director, I&A State and Local Program Office