

**NEVADA DEPARTMENT OF PUBLIC SAFETY
INVESTIGATION DIVISION
NEVADA THREAT ANALYSIS CENTER (NTAC)**


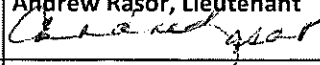
AG REVIEW BY: Samantha Ladich, Senior Deputy Attorney General 	ORIGINATION DATE: 4/22/2011	APPROVED BY: Andrew Rasor, Lieutenant 
OFFICE OF PRIMARY INTEREST: Nevada Threat Analysis Center (NTAC)	DATE EFFECTIVE: 5/3/2019	SUBJECT: Privacy, Civil Rights, and Civil Liberties Policy
PROCESSED BY: Andrew Rasor, Lieutenant	REVISION DATE: 2/21/2019	Directive Number: 19-001

TABLE OF CONTENTS

I.	PURPOSE	3
II.	POLICY APPLICABILITY	3
III.	LEGAL COMPLIANCE	3
IV.	GOVERNANCE AND OVERSIGHT	4
V.	INFORMATION GATHERING AND ACQUISITION	4
	A. Criminal Intelligence	
	B. Suspicious Activity Reports	
	C. Information Sharing Environment (ISE)	
	D. Non-Criminal Identifying Information	
VI.	INFORMATION QUALITY ASSURANCE	7
	A. Labeling	
	B. Errors/Deficiencies	
	C. Data Quality Audit	
	D. Data Audit	
VII.	COLLATION AND ANALYSIS	8
VIII.	MERGING RECORDS	9
IX.	SHARING AND DISCLOSURE	9
	A. Access	
	B. Disclosure	
	1. Disclosure to Government Agencies	
	2. Disclosure Authorized by Law	
	3. Disclosure to the Public	
	4. Disclosure of Information to an Individual	
	5. Inappropriate Uses of Disclosed Information	
X.	REDRESS	11
	A. Appeals	
	B. Complaints	
	C. Process to Review Complaints	

XI.	SECURITY SAFEGUARDS	13
	A. Privacy Officer	
	B. Secure Facility	
	C. Secure Repositories	
	D. Security Breaches	
XII.	INFORMATION RETENTION AND DESTRUCTION	14
	A. Retention of Criminal Intelligence Files	
	B. Retention of Temporary Files	
	C. Destruction	
XIII.	ACCOUNTABILITY AND ENFORCEMENT	14
	A. Information System Transparency	
	B. Accountability	
	C. Annual Audit	
	D. Enforcement	
XIV.	TRAINING	16
XV.	APPENDIX A: Terms and Definitions.....	16

I. PURPOSE

The mission of the Nevada Threat Analysis Center (NTAC) is to collect, evaluate, analyze and disseminate information and intelligence data regarding criminal and terrorist activity in the State of Nevada while following appropriate privacy and civil liberties safeguards. As such, it is the purpose of this policy to establish guidelines for the staff of the Nevada Threat Analysis Center when receiving, analyzing, and disseminating criminal intelligence and information to ensure the protection of civil liberties and personally identifiable information.

II. POLICY APPLICABILITY

All NTAC personnel, and participating agency personnel (including authorized contractors and information technology support personnel providing services to the NTAC), will comply with the privacy policy, which is in compliance with the United States Constitution, Nevada Constitution, 28 Code of Federal Regulations (CFR) Part 23, and applicable Nevada Revised Statutes (NRS). This policy applies to information that the NTAC gathers or collects, receives, maintains, stores, accesses, and discloses or disseminates to its personnel, government agencies (including the Information Sharing Environment), participating justice and public safety agencies, private contractors, private entities, and to the general public.

III. LEGAL COMPLIANCE

The NTAC will provide a printed copy of the privacy policy to all NTAC personnel and participating agency personnel who provide services to the NTAC. The NTAC will require a written acknowledgement of receipt of the privacy policy, as well as, a written agreement to comply with the privacy policy, applicable laws protecting privacy, civil rights and civil liberties, including, but not limited to:

- The United States Constitution
- The Nevada Constitution
- 28 C.F.R. Part 23 (Criminal Intelligence Systems Operating Policies)
- Nevada Revised Statutes Chapters 179A (Records of Criminal History), 239 (Public Records), 239C (Homeland Security), 241 (Public Meetings), 480 (Administration of Law Relating to Public Safety) and 603A (Security of Personal Information in Electronic Systems).

The NTAC has adopted internal operating policies that are in compliance with above listed applicable federal and state laws to protect privacy, civil rights, and civil liberties.

The NTAC Privacy Policy and its operating policies and procedures will be evaluated on an annual basis to ensure continued compliance with applicable laws, and will be completed by September 30 of each year.

IV. GOVERNANCE AND OVERSIGHT

Responsibility for the NTAC, its justice systems, operations and coordination of personnel falls within the Investigation Division of the Nevada Department of Public Safety. The Investigation Division employs a Director of NTAC to have primary responsibility for the daily operations of the center. The NTAC Director shall appoint a Privacy Officer. The Privacy Officer will have the responsibilities described in Paragraph XI, Security Safeguards.

The NTAC Advisory Committee will serve as an advisory body to the NTAC on issues related to operations, privacy and civil liberties, and policies and procedures.

The Director of the NTAC, and the designated Privacy Officer, will ensure that enforcement of procedures and sanctions outlined in this Privacy Policy are adequate and enforced and will conduct or coordinate audits and investigate violations, errors, or alleged misuse of the provisions stated in this policy.

V. INFORMATION GATHERING AND ACQUISITION

NTAC will only retain information that was obtained in a lawful manner. The following types of information may be collected by the NTAC.

A. Criminal Intelligence

The NTAC may only place information in criminal intelligence files and/or retain information that:

- Is based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved on or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, the State of Nevada or the nation and that the information is relevant to the criminal (including terrorist) conduct or activity; or
- Is based upon a possible threat to public safety or the enforcement of criminal law;
- Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime; or
- Is useful in crime analysis or in the administration of criminal justice and public safety (including topical searches); and
- The source of the information is reliable and verifiable or limitations on the quality of the information are identified; and
- Based on the source agency's good faith belief, the information was acquired in accordance with agency policy and in a lawful manner.

Information that shall be specifically excluded from criminal intelligence files includes:

- Information about individuals or organizations solely on the basis of their religious, political, or social view or activities.
- Information about individuals or organizations solely on the basis of race, ethnicity, citizenship, place of origin, age, disability, gender or sexual orientation.
- Information on an individual or group based solely on their participation in a particular non-criminal organization or lawful event.

Information related to these factors may be retained if there is a reasonable relationship or relevance to such information and the effort to detect, anticipate, or prevent criminal activity and this information is not the sole basis for retention (Reference Section XII of this policy).

The NTAC may retain information that is based on a level of suspicion that is less than “reasonable suspicion,” such as suspicious activity reports, information that is deemed reasonably indicative of terrorism, information in accordance with ISE Functional Standard 1.5.5, subject to the policies and procedures specified in this policy.

B. Suspicious Activity Reports

The NTAC will receive suspicious activity reports (SARs), which are uncorroborated reports or information that allege some form of possible criminal or terrorist activity. A suspicious activity report can result from a variety of sources, including, but not limited to:

- the public
- the media
- field interview reports
- trained law enforcement and first responders
- anonymous or confidential sources

Upon receipt of a suspicious activity report, NTAC personnel will assess the information to determine or review its nature, usability and quality. NTAC personnel will evaluate and vet the information provided to ensure:

- The information was obtained consistent with federal, state and local laws;
- Type of information, such as tips and leads, suspicious activity reports, criminal history, case support, etc.
- The nature of the source: anonymous tip, law enforcement, fusion liaison officer, private sector, citizen report, government employee, public record, open source.
- The information has the following information attached to it:
 - The name of the source agency or individual who provided the information;

- The date of submission of the information; and
- The point of contact for the information
- The information has appropriate reliability and credibility labels attached to the information.

When a suspicious activity report, a tip or lead, is received by the NTAC that does not satisfy the reasonable suspicion standard required for entry of the information into a criminal intelligence file, the NTAC may create a temporary file. Temporary files shall under no circumstances be maintained for more than one (1) year from the date of receipt.

C. Information Sharing Environment (ISE)

The NTAC is a participant in the Information Sharing Environment – Suspicious Activity Reporting (ISE-SAR) Evaluation Environment Initiative of the National Suspicious Activity Reporting (SAR) Initiative (NSI). The ISE shared space is a networked data and information repository which is under the control of submitting agencies and provides terrorism related information, applications, and services to other ISE participants. The ISE SAR process includes safeguards to ensure, to the greatest extent possible, that only information concerning individual involvement in behavior that has been determined to be consistent with criminal acts associated with terrorism will be documented and shared in the ISE shared space.

When NTAC personnel determine that a SAR has a nexus to terrorism—such as through their training; the application of the NSI Functional Standard 1.5.5; and in coordination with the ISE SAR internal NTAC policy and procedure—the SAR will be placed into the ISE shared space. Prior to placing the SAR information into the shared space, NTAC personnel will ensure the following information is included with the ISE SAR:

- 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.

D. Non-Criminal Identifying Information

Federal regulations (28 CFR Part 23) allow for the collection and storage of non-criminal identifying information in criminal intelligence systems under the following conditions:

- The information must be clearly labeled as non-criminal;
- The field in which it is entered must be searchable;
- The information must be relevant to subject's identification or criminal activity; and
- The data cannot be used as the independent basis for meeting reasonable suspicion threshold.

Political, religious, social views, associations (businesses, partnerships, etc.) or activities that are not related to suspicious conduct or activity are not permitted to be maintained.

VI. INFORMATION QUALITY ASSURANCE

The NTAC will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources; 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 [refer to Section VIII, Merging Records] has been met.

A. Labeling

At the time of retention in the system, the information will be labeled regarding its level of quality (accuracy, completeness, currency, and confidence related to verifiability and reliability). The labeling of retained information will be evaluated by the NTAC or the originating agency when new information is gathered that has an impact on confidence (source reliability and content validity) in previously retained information.

B. Errors/Deficiencies

When errors and/or deficiencies are identified, the NTAC will correct the alleged errors and deficiencies or refer them to the originating agency, in a timely manner, and correct, delete, or refrain from using protected information found to be erroneous or deficient.

C. Data Quality Audit

The NTAC will conduct periodic data quality reviews of information it originated and make every reasonable effort to ensure that the information will be corrected or deleted from the system, or not used when:

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

Originating agencies external to the NTAC are responsible for reviewing the quality and accuracy of the data provided to the center. When identified, the NTAC will notify the appropriate contact person in the originating agency, in writing or through electronic means, if data is alleged suspected or found to be inaccurate, incomplete, out of date or unverifiable.

The NTAC will use written or electronic notification to inform recipient agencies when information previously provided to the recipient agency is deleted or changed by the center because the information is 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.

D. Audit Trail

The NTAC will make use of an audit trail that provides a sufficient amount of information to establish:

- when information or events occurred
- the source(s) of the information or event
- an outcome or disposition of the information or event

VII. COLLATION AND ANALYSIS

Information acquired or received by the NTAC, or accesses 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.

Information subject to collation and analysis is information as defined and identified in Section V, Information Gathering and Acquisition.

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

- Further crime prevention (including terrorism), enforcement, force deployment, or prosecution objectives and priorities established by the NTAC and;
- 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.

The NTAC requires that all analytical products be peer reviewed, and when practicable, approved by a supervisor or the Privacy Officer, to ensure that the product provides appropriate privacy, civil rights and civil liberties protection prior to dissemination or sharing by the NTAC.

VIII. MERGING RECORDS

Records about an individual or organization from two or more sources will not be merged by the NTAC unless there is sufficient identifying information to reasonably conclude that the information is about the same individual or organization. The set of identifiers sufficient to allow merging records will consist of all available attributes that can contribute to a higher accuracy of match.

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

IX. SHARING AND DISCLOSURE

A. Access

Credentialed, role based access criteria will be used by the NTAC, to control:

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

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

B. Disclosure

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

1. Disclosure to Government Agencies

Access to, or the disclosure of records retained by the NTAC, will be provided only to persons within the NTAC or in other governmental agencies who are authorized to have access and only for legitimate law enforcement, public protection, public prosecution, public health, or justice purposes and only for the performance of official duties in accordance with law and procedure applicable to the agency for the person is working. An audit trail sufficient to allow the identification of each individual who modified information retained by the center and the nature of the information accessed will be kept by the center pursuant to the NTAC retention policy.

Agencies external to the NTAC many not disseminate information accessed or disseminated from the NTAC without approval from the center Director or other originator of the information.

2. Disclosure Authorized by Law

Information gathered or collected and records retained by the NTAC 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 identification of each individual who requested, accessed or received information retained by the NTAC; the nature of the information requested, accessed or received; and the specific purposes will be kept for no more than five years by the NTAC.

3. Disclosure to the Public

Information gathered or collected, and records retained by the NTAC, 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 NTAC, and the nature of the information accessed, will be kept by the NTAC pursuant to the NTAC retention policy.

There are several categories of records that will ordinarily not be provided to the public. The following is not meant to be an exhaustive list, but serves as examples of records that not be subject to public disclosure:

- Records required to be kept confidential pursuant to Nevada law.
- Information that meets the definition of "classified information" as the term is defined in the National Security Act, Public Law 235, Section 606 and in accord with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal and Private Sector Entities, August 18, 2010.
- Investigatory records of law enforcement agencies.
- A record or part of a record the public disclosure of which would have reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack, as determined by the Governor in an Executive Order. This includes a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism, vulnerability assessments, risk planning documents, needs assessments, and threat assessments. (NRS 239C. 210)
- Protected federal, state, local, or tribal records that were originated and controlled by another agency and were shared with the NTAC on the condition of confidentiality and non-disclosure.

4. Disclosure of Information to an Individual

Upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity and subject to the conditions specified in the next paragraph, an individual may be entitled to know the existence of, and to review the information about him or her, that has been gathered and retained by the NTAC.

The existence, content and source of the information will not be made available by the NTAC 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 §23.20(e).
- Disclosure is not allowed by state law, regulation, and/or federal law.
- The NTAC or user agency did not originate, or does not otherwise have the right to disclose, the information pursuant to a separate information sharing agreement. In such a case, the NTAC or the user agency will refer the matter to the originating agency or the agency with a right to disclose the information.

5. Inappropriate Uses of Disclosed Information

Information gathered or collected and records retained by the NTAC will not be:

- Sold, published, exchanged, or disclosed for commercial purposes.
- Disclosed published without prior notice to the originating agency that such information is subject to the 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.

X. REDRESS

If an individual requests correction of information originating with the NTAC that has been disclosed, the NTAC's Privacy Officer, or designee, will inform the individual of the procedure for requesting and considering requested corrections, including appeal rights, if requests are denied in whole or in part. A record will be kept of all requests for corrections and the resulting action, if any, pursuant to the NTAC retention policy.

A. 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 the NTAC or 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.

B. Complaints

An individual may file a complaint with the NTAC concerning the accuracy or completeness of terrorism related protected information that:

- Is exempt from disclosure,
- Has been or may be shared through the ISE
 - Is held by the NTAC; and
 - Allegedly has resulted in demonstrable harm to the complainant,

Complaints will be received by the NTAC's Privacy Officer, or designee, at the following address: Privacy Officer, Nevada Threat Analysis Center, 2478 Fairview Drive, Carson City, NV 89701. The Privacy Officer can also be contacted at: NTAC-PrivacyOfficer@dps.state.nv.us.

The Privacy Officer, or designee, will acknowledge the receipt of the complaint and inform the complainant that it will be reviewed but will not confirm the existence or non-existence of the information, unless otherwise required by law.

C. Process to Review Complaints

All information held by the NTAC that is the subject of a complaint will be reviewed within thirty (30) days of receipt, and confirmed or corrected/purged, if determined to be inaccurate or incomplete (to include incorrectly merged information or information determined to be out of date). If there is no resolution within thirty (30) days, the NTAC will not share the information until such time as the complaint has been resolved. A record will be kept by the NTAC of all complaints and the resulting action taken in response to each of the complaints.

If the information did not originate with the center, the Privacy Officer, or designee, will notify the originating agency in writing or electronically within ten (10) days of receipt. And upon request, the Privacy Officer, or designee, will assist such agency to correct and identified data/record deficiencies, purge the information, or verify that the record is accurate.

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

XI. SECURITY SAFEGUARDS

A. Privacy Officer

The Nevada Department of Public Safety will designate an individual trained to serve as the NTAC's Privacy Officer. The Privacy Officer will have the following primary responsibilities:

- Adherence to the NTAC Privacy Policy;
- Address alleged errors and violations of the NTAC Privacy Policy;
- Coordinate complaint resolution under the NTAC's Redress Policy;
- Ensure adherence to the provisions of the Information Sharing Environment privacy guidelines; and,
- Arrange privacy and civil liberties training for the NTAC personnel and participating agencies.

B. Secure Facility

The NTAC will operate in a secure facility protected from external intrusion. 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.

C. Secure Systems

Access to the NTAC information will be granted only to the 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.

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

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

- Queries made to the NTAC's data applications will be logged into the data system identifying the user initiating the query.
- The NTAC will utilize a log to maintain audit trails of requested and disseminated information.

D. Security Breaches

The NTAC 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 individual. The notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or any measures necessary to determine the scope of the release of information and, if necessary, to reasonably restore the integrity of any information system affected by this release.

The NTAC will immediately notify the originating agency from which the center received personal information of a suspected or confirmed breach of such information.

XII. INFORMATION RETENTION AND DESTRUCTION

A. Retention of Criminal Intelligence Files

All applicable information will be reviewed for record retention (validation or purge) by the NTAC at least every five (5) years, as provided by 28 CFR Part 23. The NTAC conducts quarterly reviews and ongoing maintenance to validate or purge information.

When information has no further value or meets the criteria for removal according to the NTAC retention and destruction policy, or according to applicable law, it will be purged, destroyed, and deleted or returned to the submitting (originating) agency.

B. Retention of Temporary Files

Temporary files shall under no circumstances be maintained for more than one (1) year from the date of receipt.

C. Destruction

The NTAC will delete information or return it to the originating agency once its retention period has expired, as provided by this policy. No approval will be required from the originating agency before information held by the NTAC is destroyed or returned in accordance with this policy, or as otherwise agreed upon with the originating agency or in a participation or membership agreement.

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

XIII. ACCOUNTABILITY AND ENFORCEMENT

A. Information System Transparency

The NTAC will be open with the public in regard to information and intelligence collection practices. The center's privacy policy will be provided to the public for review, made available upon request and posted at www.ntacnv.org. Requests for a copy of the privacy policy can be made to the NTAC Privacy Officer at the following email address: NTAC-PrivacyOfficer@dps.state.nv.us.

The NTAC's Privacy Officer will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights and civil liberties protections in the information system maintained or accessed by the center. The NTAC Privacy Officer can be reached at the following email address: NTAC-PrivacyOfficer@dps.state.nv.us.

B. Accountability

The NTAC will maintain an audit trail of accessed, requested, or disseminated information. An audit trail will be kept for not more than five years. The audit trail will include the requests to access information and of what information is disseminated to each person in response to the request.

The NTAC will provide annual center personnel training to reinforce applicable laws and policies. The NTAC will adopt and implement procedures to evaluate the compliance of users with this policy and with applicable law, to include, a review of logging access to NTAC information systems and periodic auditing of user compliance. A record of the audits will be maintained by the Privacy Officer.

C. Annual Audit

The NTAC will annually conduct an audit and inspection of the information and intelligence contained in its information system(s). The audit will be conducted by the center's Privacy Officer. The audit will be conducted in such a manner as to protect the confidentiality, sensitivity and privacy of the center's information and intelligence system(s). A record of the audits will be maintained by the NTAC Privacy Officer.

The Privacy Officer will review the provisions protecting privacy, civil rights and civil liberties contained in this policy annually and recommend updates, as needed, to the NTAC Director in responses to applicable law, technology, the use of the information systems and public expectations.

D. Enforcement

If center personnel, a participating agency, or an authorized user is found to be in noncompliance with the provisions of the policy regarding the gathering, collection, use, retention, destruction, sharing, classification, or disclosure of information, the Director of the NTAC may:

- Suspend or discontinue access to information.
- Apply administrative and/or legal actions or sanctions as consistent with department rules and regulations, applicable law, or as provided in agency/center personnel policies.
- request that the relevant agency, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy provisions if the user is from an agency external to the agency/center.

The NTAC 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 personnel violating the center's privacy policy.

XIV. TRAINING

The NTAC will require the following individuals to participate in training programs regarding implementation of, and adherence to, the privacy policy prior to granting access to the center:

- All assigned personnel to the center.
- Staff in other public agencies or private contractors providing services to the center.

The NTAC 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.

The NTAC's privacy policy training will include:

- Purposes of the privacy, civil rights and civil liberties protection policy.
- Substance and intent of the provisions of the policy relating to the 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 system 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 and possible penalties for policy violations, including possible transfer, dismissal, criminal liability and immunity, if any.

XV. APPENDIX A: TERMS AND DEFINITIONS

A. Authorized persons: NTAC personnel, sworn police officers, and other criminal justice

administrative personnel granted access to NTAC intelligence and information in the furtherance of their official duties.

- B. **Authorized users:** NTAC personnel, sworn police officers, and other criminal justice administrative personnel who meet certain qualifications outlined in this policy.
- C. **Civil Rights:** Refers to the government's 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.
- D. **Criminal Intelligence:** Information that has been processed – collected, evaluated and analyzed – to be used in connection with and in furtherance of law enforcement investigative purposes. It includes information that relates to an individual, organization, business, or group reasonably suspected of being involved in the actual or attempted planning, organizing, financing, or the committing of criminal acts (criminal intelligence information). It may include general threat information not necessarily directed at a specific arrest or prosecution.
- E. **Criminal Intelligence Files:** Criminal intelligence information that has been collected, processed, retained in a criminal intelligence information file, and that may be shared within the law enforcement community in the performance of law enforcement activities.
- F. **Director:** As used in this document, unless designated otherwise, refers to the Nevada Department of Public Safety sworn officer with the responsibility for all functions and activities of the Nevada Threat Analysis Center (NTAC) and its employees.
- G. **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.
- H. **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.
- I. **Information Sharing Environment Suspicious Activity Report (ISE-SAR):** A suspicious activity report that has been determined, through a two part vetting process, to have a potential terrorism nexus, i.e., to be reasonably indicative of criminal activity associated

with terrorism.

- J. **Information System:** As used in this policy “information system” means any computer equipment, computer software, procedures or technology used to collect, process, distribute or store information.
- K. **Logs:** Logs are a necessary part of an adequate security system because they are needed to ensure that data is properly tracked and that only authorized individuals are getting access to the system and the data. See Audit Trail.
- L. **Need-to-Know/Right-to-Know:**
 - 1. “Need-to-Know” is established where the prospective recipient requires access to specific information in order to perform or assist in furtherance of the agency’s valid law enforcement or public safety function.
 - 2. “Right-to-Know” is established where the prospective recipient is an employee or authorized agent of an agency that has authority to access or receive information or intelligence in furtherance of the agency’s valid law enforcement or public safety function.
- M. **National SAR Initiative (NSI):** The National SAR Initiative builds on what law enforcement and other agencies have been doing for years – gathering information regarding behaviors and incidents associated with crime and establishing a replicable process whereby suspicious activity information can be shared to help detect and prevent terrorism–related criminal activity.
- N. **Non-Criminal Identifying Information (NCI):** the names of persons, organizations, groups or businesses that are not suspected of criminal involvement, but whose identification is relevant to a criminal investigation or the identification of a criminal subject.
- O. **Persons:** As defined in NRS 0.039, “Person” is defined as: Except as otherwise expressly provided in a particular statute or required by the context, “person” means a natural person, any form of business or social organization and any other nongovernmental legal entity including, but not limited to, a corporation, partnership, association, trust or unincorporated organization. The term does not include a government, governmental agency or political subdivision of a government.
- P. **Personally Identifiable Information (PII):** Any information that can be used to uniquely identify, contact, or locate a single person or entity.
- Q. **Protected Information:** Personally identifiable information about individuals that is subject to information privacy or other legal protections under the U.S. Constitution and statutory and common laws of the United States, the Constitution of the State of Nevada, applicable state laws and local ordinances, and the provisions of this policy.

- R. 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.
- S. Purge:** The complete destruction, or return to the agency submitting such document to the NTAC, of a physical document or file and the permanent deletion from any computerized files, systems or data bases.
- T. Reasonable Suspicion:** Also known as criminal predicate, means there is enough information to establish sufficient facts to give a trained law enforcement officer or criminal investigative agency, officer, investigator, or employee a particularized and objective basis to believe that there is a reasonable probability that an individual or organization is about to be, is currently, or has been involved in a criminal enterprise or activity.
- U. Reasonably Indicative:** This operational concept for documenting and sharing suspicious activity reports takes into account the circumstances in which the observation is made, which creates in the mind of the reasonable observer, including a law enforcement officer, an articulable concern that the behavior may indicate preoperational planning associated with terrorism or other criminal activity. It also takes into account the training and experience of a reasonable law enforcement officer, in cases in which an officer is the observer or documenter of the observed behavior reported to a law enforcement agency.
- V. Redress:** Internal procedures to address disclosure, correction or appeal, from persons regarding protected information about them that is under the agency's control, including complaints regarding records that are protected from disclosure.
- W. Reliability:** The extent to which information remains consistent and dependable.
- X. Sharing:** The act of one ISE participant disseminating or giving homeland security

information, terrorism information, or law enforcement information to another ISE participant.

- Y. Suspicious Activity:** Means observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity. Examples of suspicious activity include surveillance, photography of facilities, site breach or physical intrusion, cyber-attacks, testing of security, etc.
- Z. Suspicious Activity Report (SAR):** An official document of an observed behavior that is reasonably indicative of pre-operational planning related to terrorism or other criminal activity.
- AA. Terrorism:** Terrorism is defined by Nevada Revised Statute Section 202.4415 which reads:
 - 1. "Act of terrorism" means any act that involves the use or attempted use of sabotage, coercion or violence which is intended to:
 - a. Cause great bodily harm or death to the general population; or
 - b. Cause substantial destruction, contamination or impairment of:
 - 1) Any building or infrastructure, communications, transportation, utilities or services; or
 - 2) Any natural resource or the environment.
 - 2. As used in this section, "coercion" does not include an act of civil disobedience.
- BB. 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.
- CC. Terrorism-Related Information:** In accordance with 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 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).

- DD. 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.
- EE. User:** An individual representing a participating agency who is authorized to access or receive and use a center’s information and intelligence databases and resources for lawful purposes.
- FF. User Agency:** The agency or entity authorized by the submitting agency or other authorized agency or entity to access ISE-SAR information in the SAR Data Repository, which may include analytical or operational component(s) of the submitting or authorizing agency or entity.
- GG. Validity:** The extent to which information is accurate.