ARIZONA COUNTER TERRORISM INFORMATION CENTER

PRIVACY POLICY AND PROCEDURES GUIDE

June, 2014

Privacy Policy Issuance Date:	June 3, 2014
Supersedes:	ACTIC Privacy Policy dated November, 2010
Approved by:	M.A. Orose Major Michael Orose ACTIC Director

TABLE OF CONTENTS

A. Introduction..... 3

B. Mission Statement..... 3

C. Policy Applicability and Legal Compliance..... 3

D. Governance and Oversight..... 4

E. Definitions..... 6

F. Information..... 6

G. Acquiring and Receiving Information..... 9

H. Information Quality Assurance..... 10

I. Collation and Analysis..... 11

J. Merging Records..... 11

K. Information Sharing and Disclosure 12

L. Record Review and Disclosure..... 14

M. Complaints and Corrections..... 14

N. Security and Safeguards..... 15

O. Information Retention and Destruction..... 16

P. Accountability and Enforcement..... 17

P.1 Information System Transparency..... 17

P.2 Accountability..... 18

P.3 Enforcement..... 19

Q. Training..... 19

APPENDICES

A Terms and Definitions..... 25

B Arizona Department of Public Safety Orders, Reference Materials and Federal Laws Relevant to Seeking, Retaining, and Disseminating Justice Information..... 31

C Intelligence Information vs. Criminal Information..... 33

D Criminal Intelligence File Guideline..... 35

E National Criminal Intelligence Sharing Plan Foundation for Privacy Policy Development.. 36

A. Introduction

The *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA) called for the issuance of guidelines to protect privacy and civil liberties in the development and use of the "information sharing environment" (ISE). Executive Order 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans*, provides that, "[t]o the maximum extent consistent with applicable law, agencies shall…give the highest priority to…the interchange of terrorism information among agencies…[and shall] protect the freedom, information privacy, and other legal rights of Americans in the conduct of [such] activities…"

The following policy and procedure guide implements the requirements under the IRTPA and Executive Order 13388 to protect information privacy rights and provide other legal protections relating to civil liberties and the legal rights of Americans in the development and use of the ISE.

B. Mission Statement

The mission of the Arizona Counter Terrorism Information Center (ACTIC) is to collect, evaluate, analyze, disseminate and file tactical and strategic information required to detect, deter and prosecute criminals and terrorists. The purpose of the ACTIC is to protect life and property and to anticipate, monitor, abate or prevent criminal and/or terrorist activity occurring within the State of Arizona. Fulfilling this mission requires the ACTIC to follow well-established policies, procedures, regulations and laws intended to protect the rights and privacy of Arizona's citizens.

C. Privacy Policy Applicability and Legal Compliance

1. The ACTIC has adopted internal operating policies that comply with applicable laws protecting privacy, civil rights, and civil liberties including but not limited to:

- *ACTIC Information Classification, Access, Dissemination, Storage and Destruction Policy*, IN-05012 March 24, 2006
- Arizona Department of Public Safety - General Order 3.2.10, *Sensitive and Confidential Information*
- Arizona Department of Public Safety - General Order 3.2.20, *Information/Records Management*
- Arizona Department of Public Safety - General Order 4.2.20, *Criminal Intelligence*

2. All ACTIC personnel, participating agency personnel, personnel providing information technology services to the agency, and other authorized users will comply with the

ACTIC's privacy policy concerning the information the center collects, receives, maintains, archives, accesses, or discloses to center personnel, governmental agencies (including agencies participating in the Information Sharing Environment (ISE), participating criminal justice and public safety agencies, private contractors and the general public.

3. All ACTIC personnel, participating agency personnel, personnel providing information technology services to the agency, and other authorized users will comply with all applicable laws protecting privacy, civil rights, and civil liberties.

4. The ACTIC will provide a copy of this policy to all ACTIC personnel and Terrorism Liaison Officers (TLO) who provide services and will require acknowledgement of receipt of this policy that contains a written agreement to comply with this policy and the provisions it contains.

5. The ACTIC will comply with all applicable state and federal laws, including:

- 28 Code of Federal Regulations (CFR) Part 23 - *Criminal Intelligence systems Operating Policies*
- ARS 39-121 et seq. - *Inspection of public records*
- ARS 41-1750 - *Central state repository; department of public safety; duties; funds; accounts; definitions*
- ARS 41-1803 - *Statewide critical infrastructure information system; disclosure; definition*
- ARS 41-151.18 - *Definition of records*

D. Governance and Oversight

1. Primary responsibility for the operation of the ACTIC, its justice systems, operations, coordination of personnel, the receiving, seeking, retention, evaluation, information quality, analysis destruction, sharing, or disclosure of information and the enforcement of this policy is assigned to the Director of the ACTIC.

2. The ACTIC is guided by two levels of oversight, the ACTIC Executive Management Board and the Governor's Executive Oversight Committee.

a. The ACTIC Executive Management Board is comprised of representatives from each agency participating at the ACTIC. The Executive Management Board oversees the establishment of policy and procedures at the ACTIC and provides direction when conflicts arise. The ACTIC Executive Management Board will provide management of the Privacy Policy.

b. In 2005, the Governor of Arizona signed Executive Order 2005-22 which established an ACTIC Executive Oversight Committee to oversee the operations

of the ACTIC, assuring that the ACTIC is operating efficiently and complying with all applicable responsibilities. The Governor's Executive Oversight Committee has the authority to create a working group, which can provide specific oversight for this program and any other programs relating to the civil liberties and rights of Arizona's citizens.

3. The ACTIC will utilize a command designated and trained Privacy Officer that liaises with community advocacy groups to ensure that privacy and civil rights are protected. The Privacy Officer oversees the implementation of privacy protections, ensures that the center adheres to the provisions of the ISE Privacy Guidelines and other requirements for participation in the ISE, receives and coordinates complaint resolution under the ACTIC's redress policy, and serves as the liaison for the Information Sharing Environment. It is the Privacy Officer's responsibility to ensure that privacy protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy-enhancing technologies. The Privacy Officer may be contacted at the following address:

Arizona Department of Public Safety – ACTIC
PO Box 6638
Phoenix, AZ 85005
MD 3900, Attn. Privacy Officer
602-644-5805
E-mail: acticprivacy@azdps.gov

4. The ACTIC Privacy Officer shall report to the ACTIC chain of command and the ACTIC Executive Management Board when he/she receives reports regarding alleged errors and violations of the provisions of this policy.

5. The ACTIC Director and the Privacy Officer shall ensure that enforcement procedures and sanctions outlined in **Section P.3 Enforcement** are adequate and enforced.

E. Definitions

1. Primary terms and definitions used in the ACTIC Privacy Policy and this Guide, can be found in Appendix A, *Terms and Definitions*.

F. Information

1. The ACTIC **will seek or retain information** that:

- Is based upon a criminal predicate and/or threat to public safety; **or**
- Is based upon reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or is planning criminal (including terrorist) conduct or activity that presents a

threat to any individual, the community, or the nation and the information is relevant to the criminal (including terrorist) conduct or activity; **or**

- Is relevant to the investigation and/or 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 a crime analysis and/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**
- The information was collected in a fair and lawful manner.

The ACTIC will also retain information based on mere suspicion, such as tips and leads, in addition to suspicious activity report (SAR) information based on observed behavior that is reasonably indicative of preoperational planning related to terrorism or other criminal activity. **Section F.7 will govern the ACTIC's policies and procedures for this type of information.** Appendix C has a more detailed explanation of Intelligence Information vs. Criminal Information. See also, Appendix D, *Criminal Intelligence File Defined.*

2. The ACTIC **will not seek or retain 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.

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

- The information is "Protected Information," to include "Personal Data" that pertains to all individuals (See Appendix A, Definitions) pursuant to applicable state and federal laws, Arizona Department of Public Safety General Orders and, to the extent expressly provided in this policy, organizational entities; and
- The information is subject to both state and federal laws restricting access, use, or disclosure.

4. ACTIC personnel will, upon receipt of information, assess the information to determine its nature and purpose. Personnel will assign information to categories to indicate the result of the assessment, such as:

- Whether the information is general data, tips and leads data, suspicious activity reports, or criminal intelligence information;

- The nature of the source (for example, anonymous tip, interview, public records, private sector);
- The reliability of the source (for example, reliable, usually reliable, unreliable, unknown); **and**
- The validity of the content (for example, confirmed, probable, doubtful, cannot be judged).

5. Information retained will be labeled (by record, data set, or system of records) pursuant to applicable limitations on access and sensitivity of disclosure in order to:

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

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

- New information is added that has an impact on access limitations or the sensitivity of disclosure of the information; or
- There is a change in the use of the information affecting access or disclosure limitations.

7. ACTIC personnel shall 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 reports (SARs) information. Prior to allowing access to or dissemination of the information, ACTIC personnel shall:

- Ensure that attempts to validate or refute the information have taken place and use a standard reporting format and data collection codes for SAR information.
- Assess the information for sensitivity and confidence by subjecting the information to an evaluation process to determine its credibility and value and categorize the information as unsubstantiated or uncorroborated after attempts to validate or determine the reliability of the information fail.
- Retain information for no longer than five (5) years after the calendar year entered to work a tip or lead. This will allow the ACTIC to determine its credibility and value and assign a "disposition" label (for example, undetermined or unresolved, cleared or unfounded, meets reasonable suspicion/risen to criminal intelligence) so that an authorized user knows

that status and purpose for the retention and will retain the information based upon the retention period associated with the disposition label.

- Adhere to and follow the center's physical, administrative, and technical security measures that are in place for the protection and security of tips and leads information. Tips, leads, and SARs 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.
- Allow access to or disseminate the information using the same (or a more restrictive) access or dissemination method 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).
- 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 when credible information indicates potential imminent danger to life or property.
- Store the information and include an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information.

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

9. The ACTIC will identify and review protected information originated by the center prior to sharing that information in the ISE. Further, the center will provide notice mechanisms, including but not limited to, metadata or data fields that will enable ISE authorized users to determine the nature of the protected information and how to handle the information in accordance with applicable legal requirements.

10. The following descriptive information shall be entered and electronically associated with data (or content) that is to be accessed, used, and disclosed, including terrorism-related information:

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

11. The ACTIC will apply specific labels and descriptive metadata to information that can be accessed and disseminated to indicate legal restrictions on information sharing based on information sensitivity or classification.

12. The ACTIC will keep a record of the source of all information retained by the center.

G. Acquiring and Receiving Information

1. Information gathering and investigative techniques used by the ACTIC and affiliated agencies shall comply and adhere to the following regulations and guidelines:

- 28 CFR Part 23 with regard to criminal intelligence information.
- The 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 superseding authorities provided in the federal Privacy Act; state, local, and tribal laws; or agency policy*).
- The criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) National Criminal Intelligence Sharing Plan (NCISP).
    - http://www.fas.org/irp/agency/doj/ncisp.pdf (See also Appendix-E)
- All applicable Arizona State Revised Statutes, and the applicable administrative rules, as well as any other regulations that apply to multi-jurisdictional intelligence and information databases. See Appendix B.

The ACTIC'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, appropriate center staff and participating agency staff will be trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism.

The ACTIC's SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved in activities that have been determined to be consistent with criminal activities associated with terrorism or other criminal activity will be documented and shared through the ISE. These safeguards are intended to ensure that information that could violate civil rights and civil liberties will not be intentionally or inadvertently gathered, documented, processed, and shared.

2. Information gathering and investigative techniques used by the ACTIC will use the least intrusive means necessary in each particular circumstance to gather information it is authorized to seek or retain.

3. Agencies which participate in the ACTIC and which provide information to the center are governed by the laws and rules governing those individual agencies, as well as by applicable federal and state laws.

4. The ACTIC will contract only with commercial database entities that provide an assurance that they gather personally identifiable information in compliance with local, state, tribal, territorial, and federal laws.

5. The ACTIC shall not directly or indirectly seek, accept, or retain information from;

- An individual or nongovernmental information provider who may or may not receive a fee or benefit for providing the information if the center knows or has reason to believe that the individual or information provider is legally prohibited from obtaining or disclosing the information; **or**
- The source gathered the information through prohibited means.

H. Information Quality Assurance

1. Information sought or retained by the ACTIC shall be:

- 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. (Refer to Section I. Merging Records)

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 ACTIC will investigate, in a timely manner, alleged errors and deficiencies and correct, delete, or refrain from using protected information found to be erroneous or deficient.

4. The labeling of retained information will be re-evaluated when new information is gathered that has an impact on the center's confidence (validity and reliability) in retained information.

5. The ACTIC will make every reasonable effort, through periodic data quality reviews of information gathered or collected, to ensure that the information is corrected, deleted from the system, or not used when the center learns that the information is erroneous, misleading, obsolete, or otherwise unreliable. This will include situations where it is determined that the source agency did not have authority to gather the information or provide it to the ACTIC, or used prohibited means to gather the information.

6. State and Local agencies, including agencies participating in the ISE, are responsible for the quality and accuracy of the data accessed by or shared with the center. Originating agencies providing data remain the owners of the data contributed. The ACTIC will advise the appropriate data owner, in writing, if its data is suspected or determined to be erroneous, misleading, obsolete, or otherwise unreliable.

7. The ACTIC will use written or documented electronic notification to inform recipient agencies when information previously provided by the ACTIC is deleted or changed by the center. This includes information that is determined to be erroneous, misleading, obsolete, incorrectly merged, lacks adequate context, or is otherwise unreliable.

I. Collation and Analysis

1. Information acquired by the ACTIC or accessed from other sources will only be analyzed 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 *Section F, Information.*

3. Information sought or received by the ACTIC or from other sources will be used to:

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

J. Merging 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.

K. Sharing and Disclosure

1. Credentialed, role-based access criteria and ACJIS Terminal Operator Certification will be used to control:

- Information a class of users can have access to;
- Information a class of users can add, change, delete, or print; **and**
- To whom the information can be disclosed and under what circumstances.

Dissemination lists of authorized law enforcement and government recipients will be vetted and maintained by the ACTIC Intelligence Analysis Unit (AIAU). Terrorism Liaison Officer (TLO) access to information will be vetted and maintained by the ACTIC TLO Coordinator.

The ACTIC 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, commonly accepted data collection codes and a sharing process that complies with the ISE-SAR Functional Standard for suspicious activity potentially related to terrorism.

2. Access to or disclosure of records retained by the ACTIC will only be provided ***to persons within the ACTIC 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. Access and disclosure will be limited to the performance of official duties in accordance with law and procedures applicable to the agency for which the person is working. An audit trail of access or dissemination of information to such persons will be maintained.

3. Participating agencies may not disseminate ACTIC information received from ACTIC without approval from the originator of the information.

4. Records retained by the ACTIC 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 of access by or dissemination of information to such persons will be maintained.

5. Information gathered and records retained by the ACTIC may be accessed or disseminated ***for specific purposes*** upon request by persons authorized by law to have such access and only for those users or purposes specified in the law. An audit trail will be kept for a minimum of five years after the calendar year recorded by the center. The audit trail shall include sufficient information to allow the identification of each

individual who requested, accessed, or received information retained by the ACTIC, the nature of the information requested, accessed, or received and the specific purpose for which it was requested, accessed, or received.

6. Information gathered and records retained by the ACTIC may be accessed or disclosed to a member of the public ***only*** if the information is not exempt from disclosure under Arizona law and the information is specific to the requester. Such information may *only* be disclosed in accordance with the conditions outlined below. An audit trail of all requests and of the information disclosed to a member of the public shall be maintained.

7. Information gathered and records retained by the ACTIC ***will not*** be:

- Sold, published, exchanged, or disclosed for commercial purposes;
- Disclosed or published without prior notice to the contributing agency that such information is subject to re-disclosure or publication; ***or***
- Disseminated to unauthorized persons.

8. The existence, content, and source of a record will not be made available to a member of the public when there is a legal basis for denial in accordance with Arizona law, to include ARS 39-121 et seq., ARS 41-1750 and ARS 41-1803 and associated case law. Arizona law provides exceptions to disclosure when non-disclosure serves the confidentiality, privacy or best interests of the state or when disclosure would adversely affect the ACTIC's mission to detect, deter and prosecute criminals and terrorists. Additionally, ARS 39-121 et seq. applies to those records, as defined by ARS 41-151.18, made or received by the ACTIC in connection with the transaction of public business. Thus, records which are not maintained or under the control of the ACTIC are not subject to disclosure. When a request is received, it will be reviewed to determine if any of the following situations apply:

- Non-disclosure serves the confidentiality, privacy, or the best interests of the state in accordance with interpretations of ARS 39-121 et seq.
- The record involves the statewide critical infrastructure information system and is prohibited from disclosure by ARS 41-1803
- The record is not a public record as defined by ARS 41-151.18 and therefore not subject to disclosure under ARS 39-121 et seq.
- Disclosure is prohibited by law

If any of these situations apply, or there is any other legal reason for non-disclosure, the record will not be disclosed.

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

L. Record Review

1. The ACTIC Privacy Officer will respond to all requests for review of information within a timely manner and in a form that is consistent with Arizona law including ARS 39-121 and ARS 41-1750 and with the Arizona Department of Public Safety's public records policy (See Appendix B, Arizona Department of Public Safety General Orders 3.2.10, 3.2.20, 4.2.20) The ACTIC Privacy Officer will maintain a record of all requests and of what information is disclosed.

2. The existence, content, and source of the information will not be made available to an individual when there is a legal basis for denial in accordance with Arizona law including ARS 39-121 and ARS 41-1750.

3. Complaints regarding disclosure of information retained by the ACTIC shall be directed to the ACTIC Privacy Officer at the following address:

Arizona Department of Public Safety – ACTIC
PO Box 6638
Phoenix, AZ 85005
MD 3900, Attn. Privacy Officer
602-644-5805
E-mail: acticprivacy@azdps.gov

M. Complaints and Corrections

1. If an individual has complaints or objections to the accuracy or completeness of terrorism–related protected information retained about him or her ***within a system under the ACTIC's control*** that: (a) is exempt from disclosure, (b) has been or may be shared through the ISE, and allegedly has resulted in demonstrable harm to the complainant, the ACTIC will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the ACTIC Privacy Officer at the following address:

Arizona Department of Public Safety – ACTIC
PO Box 6638
Phoenix, AZ 85005
MD 3900, Attn. Privacy Officer
602-644-5805
E-mail: acticprivacy@azdps.gov

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

2. If an individual has complaints or objections to the accuracy or completeness ***of information*** that has been disclosed to him or her, the ACTIC Privacy Officer or designee will refer the individual to the originating agency for resolution. The originating agency is responsible for consenting to the correction, removing the record, or asserting a basis for denial in accordance with law. This must be done in sufficient time to permit compliance with deadlines found within the ARS § 41-1750. A record will be kept of all complaints and correction requests and the resulting disposition by the command designated Privacy Officer.

3. To delineate ISE information from other data, the ACTIC maintains records of the ISE originating agencies the center has access to as well as by e-mail dissemination audit logs, and employs mandatory system data entry mechanisms whereby the source is identified within the information record.

4. If requests for access or corrections are denied by the ACTIC, the ACTIC will provide an explanation for the denial. The ACTIC will also provide notice of the procedure for appeal when the center has declined to provide access or modify challenged information to the satisfaction of the individual about whom the information relates.

N. Security Safeguards

1. The ACTIC Director shall designate an appropriately trained individual to be the ACTIC data systems security officer.

2. The ACTIC will operate in a secure facility protecting the facility from external intrusion.

3. The ACTIC will utilize secure internal and external safeguards against network intrusions.

4. Access to ACTIC databases from outside the facility will only be allowed over secure networks. This includes those accessed by Terrorism Liaison Officers and Field Intelligence Teams. The ACTIC will secure tips, leads, and SAR information in a separate repository system using security procedures and policies that are the same as or similar to those used for a system that secures data rising to the level of reasonable suspicion under 28 CFR Part 23.

5. The ACTIC 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 and such access and actions will be documented by automated and unalterable electronic means.

6. Access to center information will only be granted to center personnel whose position and job duties require such access and the individual has successfully completed a background check, holds the appropriate security clearance, if applicable, and has been selected, approved, and trained accordingly.

7. Queries made to the ACTIC databases will be automatically logged into the data system identifying the user initiating the query.

8. The ACTIC will utilize both manual and automated electronically created logs to maintain audit trails of requested and disseminated information.

9. To prevent public records disclosure and ensure compliance with the tenets of the Protected Critical Infrastructure Information (PCII), risk and vulnerability assessments will not be stored with other data but instead will be stored in a separate critical asset management system.

10. The ACTIC will notify an individual about whom personal information within ACTIC's control was or is reasonably believed to have been breached or obtained by an unauthorized person and access to which threatens the physical safety, reputation, or could cause financial harm to the person. The notice will be made promptly following discovery or notification of the access to the information. Such notice will be consistent with the legitimate needs of law enforcement to investigate the release, determine the scope of the release of information and, if necessary, to reasonably restore the integrity of any information system affected by this release.

O. Information Retention and Destruction

1. All criminal intelligence information will be reviewed for record retention (validation or purge) at least every five (5) years, as provided by 28 CFR Part 23.

2. All other information will be reviewed for record retention as per state statute.

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

4. The ACTIC will delete information or return it to the source, unless it is validated, every five (5) years, which will be compliant with 28 CFR Part 23.

5. Permission to destroy or return information or records will be presumed if the applicable information is not validated within the specified period, as per item (2.) above.

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

7. A record of information to be reviewed for retention will be maintained by the Regional Information Sharing Systems (RISS7) Administrator, and for appropriate system(s), notice will be given to the submitter no more than 90 days and no less than 30 days prior to the required review and validation/purge date.

P. Accountability and Enforcement

P.1 Information System Transparency

1. The ACTIC will be open with the public concerning information and intelligence collection practices. The ACTIC's privacy policy will be provided to the public for review and will be made available upon request and posted on the Department of Public Safety website.

2. The ACTIC's designated 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) and referring those that require further consideration to the appropriate authority. The Privacy Officer can be contacted at the following address:

Arizona Department of Public Safety – ACTIC
PO Box 6638
Phoenix, AZ 85005
MD 3900, Attn. Privacy Officer

602-644-5805
E-mail: acticprivacy@azdps.gov

P.2 Accountability

1. The ACTIC will provide a copy of this Privacy Policy and Procedures Guide to all ACTIC personnel and TLO's 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.

2. The ACTIC Watch Center Tips and Leads database's reports capability will be utilized to maintain an audit log of entries, queries, and requests to the ACTIC and an audit trail of disseminated intelligence and information from the Watch Center Tips and Leads database. The audit trail will be kept for a minimum of 10 years after the calendar year recorded of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.

3. All queries made to other ACTIC data systems and/or RISS7 can be initiated by validated users logged into that data system, which identifies the user initiating the query.

4. The ACTIC will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users of their systems, in provisions of this policy and applicable law. This will include designating a Privacy Officer, appointing a Privacy Committee, and developing audit practices in accordance with the appropriate guidelines. Once designated and established the Privacy Officer will monitor logging access to these systems and periodic audits of these systems, as to not establish a pattern of the audits. These audits are mandated at least quarterly, and a record of the audit will be maintained by the Director (or designee) of the ACTIC.

5. The ACTIC's personnel or other authorized users shall report violations or suspected violations of center policies relating to protected information to the center's Privacy Officer.

6. The ACTIC will conduct annual and random audits and inspections of the information contained in its criminal intelligence system when so ordered by the ACTIC Director. The audit will be conducted by a designated representative or by an independent party selected by the agency (ACTIC) or the Governor's Executive Oversight Committee which will comprise of members with proper security clearances and knowledge of intelligence collection policy and procedures. This representative or independent party has the option of conducting a random audit, without announcement, at any time and without prior notice to the ACTIC. This audit will be conducted in such a manner to protect the confidentiality, sensitivity, and privacy of the center's criminal intelligence system.

7. The ACTIC's Privacy Committee (and/or Privacy Officer) will annually review and update the provisions protecting privacy, civil rights, and civil liberties contained within this policy and make appropriate changes in response to changes in applicable law, changes in technology, changes in the purpose and use of the information systems, and changes in public expectations.

P.3 Enforcement

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

- Suspend or discontinue access to information by the center personnel, the participating agency, or the authorized user.
- Refer administrative actions or sanctions to the appropriate agency.
- If the authorized user is from an agency external to the ACTIC, request that the relevant agency, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions.
- Refer the matter to appropriate authorities for criminal prosecution, as necessary, to accomplish the purposes of the policy.

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

Q. Training

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

- All permanently assigned personnel of the center
- TLO's in their initial training phase

2. The ACTIC will provide special training to personnel authorized to share protected information in the ISE regarding the center's requirements and policies for collection, use, and disclosure of protected information.

3. The ACTIC's privacy policy training program will cover:

- Purposes of the privacy, civil rights, and civil liberties protection policy;

- Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the ACTIC;
- How to implement the policy in the day-to-day work of the user, whether a paper or systems user;
- The impact of improper activities associated with infraction accessible within or through the agency;
- Mechanisms for reporting violations of center privacy-protection policies; ***and***
- The nature and possible penalties for policy violations, including possible transfer, dismissal, criminal liability, if any.

ACTIC Personnel are hereby directed to follow their parent agencies' procedures concerning privacy and civil rights issues and report any situation that conflicts with this guide to the ACTIC Privacy Officer for resolution before taking any action.

Appendix A
Terms and 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. For data access, access is usually specified as read-only access and read/write access. With regard to the Information Sharing Environment (ISE), access refers to the business rules, means, and processes by and through which ISE participants obtain terrorism related information, to include homeland security information, terrorism information, and law enforcement information acquired in the first instance by another ISE participant.

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

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 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/Center—Agency/Center refers to the ACTIC and all participating Federal, State, Local and Tribal agencies of the ACTIC.

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

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

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

Authorization—The process of granting a person, computer process, or device with access to certain information, services, or functionality. Authorization is derived

from the identity of the person, computer process, or device requesting access that is verified through authentication. See Authentication.

Biometrics—Biometrics methods can be divided into two categories: physiological and behavioral. Implementations of the former include face, eye (retina or iris), finger (fingertip, thumb, finger length or pattern), palm (print or topography), and hand geometry. The latter includes voiceprints and handwritten signatures.

Civil Rights—The term "civil rights" is used to imply that the state has a role in ensuring 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 upon government to promote equality. More specifically, they are the rights to personal liberty guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments and by acts of Congress.

Civil Liberties—Civil liberties are fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights, the first ten Amendments to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference. Generally, the term "civil rights" involves positive (or affirmative) government action, while the term "civil liberties" involves restrictions on government.

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

Computer Security—The protection of information assets using technology, processes, and training.

Confidentiality—The obligation of individuals and institutions to protect private information under their control and maintain its privacy once it has been disclosed to them. See *Privacy*.

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

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

Critical Infrastructure—means the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public

health or safety, or any combination thereof. State statutes related to critical infrastructure can be found in Arizona Revised Statutes, Title 41, §1801 through 1805.

Data—Inert symbols, signs, or measures.

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

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

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

Electronically Transmitted—Information exchanged with a computer using electronic media, such as the movement of information from one location to another by magnetic or optical media, transmission over the Internet, intranet, extranet, leased lines, dial-up lines, private networks, telephone voice response, and faxback systems. It does not include faxes, telephone calls, video teleconferencing, or messages left on voice mail.

Evidential Intelligence — Information that is factual and precise, which could be presented in court, used to develop a strategic report, or may have tactical value and be currently useful in a case being prosecuted.

Fair Information Practices—The Fair Information Practice Principles (FIIPs) form the framework for privacy policy at the United States Department of Homeland Security. The FIIPs were developed around commercial transactions and the trans-border exchange of information. They provide a straightforward description of underlying privacy and information exchange principles, as well as a simple framework for the legal analysis that needs to be done with regard to privacy in integrated justice systems. The eight FIIPs are:

1. Transparency
2. Individual Participation
3. Purpose Specification
4. Data Minimization
5. Use Limitations
6. Data Quality and Integrity
7. Security
8. Accountability and Auditing

Firewall—A security solution that segregates one portion of a network from another portion, allowing only authorized network traffic to pass through according to traffic-filtering rules.

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

Homeland Security Information—As defined in Section 482(f)(1) of the Homeland Security Act, homeland security information means any information possessed by a federal, state, local, or tribal agency that relates to (A) a threat of terrorist activity; (B) the ability to prevent, interdict, or disrupt terrorist activity; (C) the identification or investigation of a suspected terrorist or terrorist organization or any person, group, or entity associated with or assisting a suspected terrorist or terrorist organization; or (D) a planned or actual response to a terrorist act.

Identification—A process whereby an individual or real-world entity is recognized and its identity established. Identity is operationalized in the abstract world of information systems as a set of information about an individual or entity that differentiates it from other similar individuals or entities. The set of information may be as small as a single code, specifically designed as an identifier, or a compound of such data as a given and family name, date of birth, and address. An organization's identification process comprises the acquisition of the relevant identifying information.

Indicative Intelligence — Information that suggests any new developments or operations by organized criminal groups. The information may be fragmentary and difficult to substantiate immediately.

Individual Responsibility—The accountability for something within one's power, control, or management. Since a privacy notice is not self-implementing, an individual within an organization's structure is also assigned responsibility for enacting and implementing the notice.

Information—Unevaluated material obtained from observations, communications, reports and pictures. 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 three general areas: general data, tips and leads data, and criminal intelligence data.

Information Quality—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.

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

Intelligence-Led Policing —a collaborative enterprise based on improved operations in information gathering, community-oriented policing and problem solving.

Invasion of Privacy—an intrusion on one's solitude or into one's private affairs, public disclosure of embarrassing private information, publicity that puts one in a false light to the public, or appropriation of one's name or picture for personal or commercial advantage. **See also Right to Privacy.**

Law—As used in 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—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.

Lawful Permanent Resident—A foreign national who has been granted the privilege of permanently living and working in the United States.

Least Privilege Administration—A recommended security practice in which every user is provided with only the minimum access needed to accomplish the tasks they are authorized to perform.

Logs—the documentation of tracking that shows only authorized individuals are getting access to the data. **See also Audit Trail.**

Maintenance of Information—means the manner in which information is retained and destroyed. The maintenance of information applies to all forms of information storage. This would include electronic systems (for example, databases) and non-electronic storage systems (for example, filing cabinets). To meet access requirements, an organization is not required to create new systems to maintain

information or maintain information beyond a time when it no longer serves an organization's purpose.

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

Need to Know—As a result of jurisdictional, organizational, or operational necessities, access to sensitive information or intelligence is necessary for the conduct of an individual's official duties as part of an organization that has a right to know the information in the performance of a law enforcement, homeland security, or counter-terrorism activity, such as to further an investigation or meet another law enforcement requirement.

Non-Repudiation—A technique used to ensure that someone performing an action on a computer cannot falsely deny that they performed that action. Non-repudiation provides undeniable proof that a user took a specific action, such as transferring money, authorizing a purchase, or sending a message.

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

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

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

- Personal characteristics (such as height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation, place of birth, mother's maiden name, distinguishing features, and biometrics information, such as fingerprints, DNA, and retinal scans).
- A unique set of numbers or characters assigned to a specific individual (including name, address, phone number, social security number, e-mail address, driver's license number, financial account or credit card number and associated PIN number, Automated Integrated Fingerprint Identification System [AIFIS] identifier, or booking or detention system number).
- Descriptions of event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records).

- Descriptions of location(s) or place(s) (including geographic information systems [GIS] locations, electronic bracelet monitoring information, etc.).

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

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

Privacy Policy—a written, published statement that articulates the position of an organization on how it handles the personally identifiable information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, dissemination, and access. The purpose of the privacy policy is to articulate that the agency will adhere to those legal requirements and agency 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 finding appropriate balances between unsanctioned intrusions and multiple competing interests, such as justice information sharing.

Protected Information—includes personal data about individuals that is subject to information privacy or other legal protections by law, including the U.S. Constitution and the Arizona constitution; applicable law of the United States, including civil rights laws and 28 CFR Part 23; applicable state and tribal constitutions; and State, Local and Tribal laws, ordinances, and codes. Protection may also be extended to organizations by ACTIC policy or state, local, or tribal law.

Public—Public includes:

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

- Entities that seek, receive, or disseminate information for whatever reason, regardless of whether 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 in the operation of the justice information system, and agency in the operation of the justice information system; **and**
- Public agencies whose authority to access information gathered and retained by the agency is specified in law.

Public Access—the information that can be seen by the public, that is, information whose availability is not subject to privacy interests or rights.

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

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

Retention—Refer to "Storage."

Right to Know—Based on having legal authority or responsibility or pursuant to an authorized agreement, an agency or organization is authorized to access sensitive information and intelligence in the performance of a law enforcement, homeland security, or counterterrorism activity.

Right to Privacy—the state of being free from intrusion or disturbance in one's private life or affairs, in the absence of some reasonable public interest in a person's activities. Invasion of the right to privacy can be the basis for a lawsuit for damages against the person or entity violating that right.

Role-Based Authorization—A type of authorization that uses roles to determine access 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 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.

Strategic Intelligence—Information that is collected over time, collated, analyzed and used by command level personnel of an agency in planning allocation of their resources.

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 IT industry than meaning (2.)
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.

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 facilities, site breach or physical intrusion, cyber attacks, testing of security, etc.

Suspicious Activity Reports (SARs)—the 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.

Tactical Intelligence—Information that indicates that criminal activity is taking place, or is about to take place, which may require immediate enforcement action. Enforcement action may lead to an arrest or further information gathering.

Terrorism Information—Consistent with Section 1016(a) (4) of IRTPA, all information relating to:

(A) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material 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 Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). 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) 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—Uncorroborated report or information generated from inside or outside the agency that alleges or indicates some form of possible criminal activity. Tips and leads can also be referred to as suspicious incident reports (SIRs), suspicious activity reports (SARs), and/or field interview reports (FIRs). Tips and leads information does not include incidents that do not have an offense attached, criminal history records, or CAD data. A tip or lead can result from a variety of sources, including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information has some suspicion or mere suspicion attached to it, but without further inquiry or analysis, it is unknown whether the information is accurate or useful. Tips and leads information hangs between being of no use to law enforcement and being extremely valuable if time and resources are available to determine its meaning. Tips and leads information is maintained in a secure system similar to data that rises to the level of reasonable suspicion.

Appendix B

Arizona Department of Public Safety General Orders, Reference Materials and Federal Laws Relevant to Seeking, Retaining, and Disseminating Justice Information

The following is a listing of federal/state laws and Arizona Department of Public Safety Policies and General Orders reviewed during the development of the ACTIC Privacy Policy. The list is arranged in alphabetical order by popular name.

Automated Critical Asset Management System (ACAMS)
http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf
http://www.dhs.gov/xlibrary/assets/pcii_final_rule_federal_register9-1-06-2.pdf
ACTIC Information Classification, Access, Dissemination, Storage and Destruction Policy, IN 05012 dtd March 24, 2006
Arizona Department of Public Safety General Order 3.2.10, Sensitive and Confidential Information dated November 18, 2002.
Arizona Department of Public Safety General Order 3.2.20, Information/Records Management dated July 1, 2006. (http://www.azdps.gov/Services/Records/)
Arizona Department of Public Safety General Order 4.2.20, Criminal Intelligence dated May 1, 2002.
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 Non-criminal 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
IALEIA/LEIU Intelligence 2000 – *Reviewing the Basic Elements, A Guide for Intelligence Professionals* **-Intelligence 2000: Revising the Basic Elements, Marilyn B. Peterson, Bob Morehouse and Richard Wright, editors (LEIU), 2000, ISBN 0-970-6887-0-9**
Indian Civil Rights Act of 1968, 25 U.S.C. § 1301, United States Code, Title 25, Chapter 15, Subchapter I, § 1301
IRTPA, as amended by the 9/11 Commission Act enacted on August 3, 2007 (P.L. 110-53), Information Sharing Environment Privacy Guidelines 2006 (2009):
http://www.ise.gov/docs/privacy/PrivacyGuidelines20061204.pdf
http://www.dhs.gov/xlibrary/assets/privacy/privacy_crcl_guidance_ise_2009-01.pdf
National Child Protection Act of 1993, Pub. L. 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
National Criminal Intelligence Sharing Plan (DOJ – NCISP October 2003)
http://www.fas.org/irp/agency/doj/ncisp.pdf
OMB Memorandum M 07-16 (May 2007).
http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf
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 No. 107-56 (October 26, 2001), 115 Stat. 272

Appendix C
Intelligence Information vs. Criminal Information

Within the law enforcement community, it is important to differentiate between criminal investigations and intelligence investigations, and the prevalent distinctions between criminal record information and intelligence record information.

Criminal investigations and intelligence investigations are similar in that they entail the application of basic investigative skills against known or suspected criminal activity. Intelligence investigations are a proactive crime prevention effort and a viable part of community oriented or intelligence led policing.

The main difference between the two categories and the manner in which their results are documented and filed is essentially a matter of scope and degree rather than content.

Generally, criminal investigations are initiated based on a specific complaint. Such complaints are ordinarily investigated to an acceptable conclusion, i.e., the perpetrator is arrested and prosecuted - or the complaint, upon investigation, is determined to be groundless and no criminal violation occurred. Criminal investigations are reactive in nature and involve specific criminal violations. Specific victims are usually identified at the outset. Criminal investigations proceed from the specific to the general, or general to the specific. It may lead to one perpetrator or an organized group of perpetrators involved in other types of crimes. Its focus is toward "hard" or provable information, which is designed for presentation in court.

Intelligence investigations are sometimes predicated on a specific complaint however, this is not usually the case. More often, intelligence investigations are initiated upon receipt of information that a broad criminal activity exists. The intelligence investigation is proactive and attempts to proceed from this general complaint to the specific, by actually verifying the existence of the criminal activity and identifying the various members as well as their methods of operation. Once this has been accomplished, the details are furnished to the appropriate criminal investigation unit for enforcement action.

In the model intelligence unit, the intelligence investigative function does not entail an enforcement role. The reason for avoiding the arrest situation is twofold. First, to reduce or minimize the extent to which the intelligence detectives become widely known. Second, and perhaps more importantly, is to avoid placing enforcement requirements on the intelligence unit, which would interfere with their primary intelligence function, the collection of information.

Reports of intelligence investigations may contain specific details of criminal matters identical to the reports prepared during normal criminal investigations. The basic difference is that intelligence investigations usually begin because of general information and must be documented and filed so that it is retrievable later on.

The initial information the intelligence unit receives is usually non-specific and would not meet the standard criteria for filing in a normal criminal investigative file. As the intelligence investigation proceeds, additional reports may be generated. The intelligence database affords a

separate location where such non-specific, essential information can be retained, analyzed, compared and disseminated to other bona fide subscribers. The intelligence database also enables the storage of information by crime category, such as arson, auto theft, motorcycle gangs, narcotics, terrorism, prison gangs, etc., which is suited for analytical exploitation. Analysis of a volume of rather seemingly unrelated information may well disclose the existence of a new organized group or a new Modus Operandi (or Method of Operation.) This proactive role of the intelligence unit is accomplished through the analysis of information already in file.

It is difficult for a criminal intelligence unit to determine or predict criminal threats to their jurisdiction if sources do not exist for all segments of a community. Intelligence detectives must collect information which, when compared with previously collected data and then analyzed, will result in the development of intelligence.

Intelligence in the true sense relates to advance knowledge of impending events. Information pertains to events, facts or data that is being collected, but not applied knowledge.

Intelligence units are the focal point for the investigation of organized criminal activity. These groups are mobile and their members and associates are in a constant state of flux. Tracking these groups is a long-term proposition that requires a standardized record keeping procedure to retain pertinent information.

The national standard definitions of various types of crime-related information are as follows:

Criminal Justice Information
Information collected by criminal justice agencies needed for the performance of their legally authorized and required functions. This is the broadest information term, and includes Criminal History Record Information and investigative and intelligence information. It does not include personnel or administrative records used for agency operations or management.

Intelligence and Investigative Information
Information compiled in an effort to anticipate, prevent or monitor possible criminal activity, or compiled in a course of investigation of known or suspected crimes.

Criminal History Record Information
Information collected by criminal justice agencies on individuals, consisting of identifiable descriptions and notations of arrests, detentions, indictments, information, or other formal criminal charges, and any disposition(s) arising from sentencing, correctional supervision, and release.

Computerized Criminal History
A computerized criminal history system (CCH) is criminal history record information concerning an identified offender or an alleged offender contained in an automated file. CCH is also a common name for the program of automated files maintained by the FBI and states, for the national and state exchange of criminal history record information. A computerized criminal history does not include fingerprints, but entry of the identifying data from the fingerprint card and criminal reports.

Appendix D
Criminal Intelligence File Defined

Criminal intelligence information is recorded data that has been evaluated to determine that it is relevant to the identification of individual(s) who, and group(s) or organization(s) which, are reasonably suspected of engaging in criminal activity.

A criminal intelligence file consists of stored information on the activities and associations of:

A. Individuals who:

• are reasonably suspected of being involved in the actual or attempted planning, organizing, financing, or commission of criminal acts; or
• are reasonably suspected of being involved in criminal activities with known or suspected crime figures.

B. Organizations, businesses, and groups that:

• are reasonably suspected of being involved in the actual or attempted planning, organizing, financing or commission of criminal acts; or
• are reasonably suspected of being illegally operated, controlled, financed, or infiltrated by known or suspected crime figures for use in an illegal manner.

C. General crimes that are documented in a Criminal Intelligence File include but are not limited to:

Bribery	Mayhem – Disturbing the Peace
Burglary	Money Laundering
Counterfeiting	Murder
Criminal Extremism	Narcotics – Distribution / Manufacture
Espionage	Pornography
Extortion	Prostitution
Fencing	Possession or Use of Weapons and Explosives for Unlawful Means
Forgery	Public Corruption
Fraud	Robbery
Funding of Violent Activity	Smuggling
Gambling	Stolen Securities
Identity Theft	Terrorism
Labor Racketeering	Trafficking – Humans / Weapons / Narcotics
Loan Sharking	Treason

Appendix E
National Criminal Intelligence Sharing Plan (NCISP)
(EXCERPT)
Foundation and Recommendation for Privacy Policy Development: "The need to ensure that individuals' constitutional rights, civil liberties, civil rights, and privacy interests are protected throughout the intelligence process"

The protection of individuals' privacy and constitutional rights is an obligation of government officials and is crucial to the long-term success of criminal intelligence sharing. Protecting the privacy and constitutional rights of individuals, while at the same time providing for homeland security and public safety, will require a commitment from everyone in the system - from line officers to top management.

For the purposes of this document, the term *constitutional rights* refer to those rights that an individual derives from the Constitution of the United States. Constitutional rights are the strongest protection from improper government conduct against an individual. Unlike other legal rights, constitutional rights cannot be changed by a statute. They can only be altered by amending the Constitution.

The term *civil liberties* refers to 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 in relation to the specific freedoms enumerated in the Bill of Rights.

The term *civil rights* is used to imply that the state has a role in ensuring all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of race, religion, sex, or other characteristics unrelated to the worth of the individual. Civil rights are, therefore, obligations imposed upon 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. Generally, the term civil rights involve positive (or affirmative) government action, while the term civil liberties involve restrictions on government.

The term *privacy* refers to individuals' interests in preventing the inappropriate collection, use, and release of personally identifiable information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. The U.S. Constitution does not explicitly use the word "*privacy*," but several of its provisions protect different aspects of this fundamental right.[17]

Although there does not exist an explicit federal constitutional right to an individual's privacy,[18] privacy rights have been articulated in limited contexts by the U.S. Supreme Court.[19] Privacy protections are numerous and include protection from unnecessary or unauthorized collection of

personal information (e.g., eavesdropping), public disclosure of private facts, and shame or humiliation caused by release of personal information. The National Criminal Intelligence Sharing Plan supports policies that will protect privacy and constitutional rights while not hindering the intelligence process. When agencies are reviewing or formulating their policies, it may be helpful to view the intelligence process as a series of discretionary decisions.[20]

At each step, a decision must be made, usually involving a choice from among several possible alternatives. Consider, for example, how a criminal intelligence unit might respond to an unsolicited, anonymous tip alleging that a particular individual is engaged in criminal activity. Should the unit query various police records systems in an effort to learn more about the "suspect?" Should they query commercial or other public record databases? Should they conduct surveillance of the "suspect?" or should they disseminate the information to other law enforcement agencies in an effort to learn more about the person? What kinds of additional records are created when these actions are taken? Then, after those actions are taken, additional decisions must be made regarding what information and how much, if any, to store about the "suspect" in the criminal intelligence files. Violations of privacy and constitutional rights may potentially occur when choices are selected from these various alternatives. In order to be effective, a policy that addresses the protection of individual privacy and constitutional rights should attempt to eliminate the unnecessary discretion in the decision-making process, guide the necessary discretion, and continually audit the process to ensure conformance with the policy goals.[21]

17 For early references to this principle, see Samuel Warren and Louis Brandeis. 1890 (December 15). "The Right to Privacy." *Harvard Law Review* 4(5): 193-220.

18 The most closely related constitutional right is that under the Fourth Amendment, which prohibits unreasonable search and seizure of individuals and their houses, papers, and effects. U.S. Constitution Amendment IV. Some states, such as California, recognize a right to privacy in their state Constitutions. See California Constitution article 1, §1 (West 1983).

19 National Criminal Justice Association. 2002 (September). *Justice Information Privacy Guideline: Developing, Drafting, and Assessing Privacy Policy for Justice Information Systems*. Washington, DC: NCJA, pp. 18-19.

20 This framework was used by Wayne LaFave, who observed, "It is helpful to look at the total criminal justice system as a series of interrelated discretionary choices." (LaFave, 1965). *Arrest*. Boston, MA: Little Brown. Like any model or framework, it is valuable not because it is the only way or the right way to describe the process, but because of the insights that it provides.

21 The framework for regulating discretionary decisions (i.e., eliminating unnecessary discretion, and confining, structuring, and checking necessary discretion) through administrative rule making and agency policies is derived from Kenneth Culp Davis. (Davis, 1971). *Discretionary Justice: A Preliminary Inquiry*. Urbana, IL: University of Illinois; and (Davis, 1975). *Police Discretion*. St. Paul, MN: West Publishing Company.