OIFC 17

PRIVACY POLICY

August 06, 2009

I. Purpose Statement

A. The Oklahoma Information Fusion Center (OIFC) was authorized by Governor Brad Henry on October 16, 2007, by Executive Order 2007-41, to detect, prevent, investigate, and respond to criminal and terrorist activity. The mission of the OIFC is to collect, evaluate, analyze and disseminate information and intelligence data regarding criminal and terrorist activity to federal, state, local and tribal law enforcement agencies, other Fusion Centers, and to the public and private entities as appropriate, while following the *Fair Information Practices* to ensure the rights and privacy of citizens.

B. OIFC's Privacy Policy applies to all individuals and organizations. The purpose of OIFC's Privacy Policy is to ensure that OIFC personnel with direct access to OIFC information comply with federal, state, local and tribal laws, OIFC's policies and procedures, and assists its authorized users in:

1. Increasing public safety and improving national security.
2. Minimizing the threat and risk of injury to specific individuals.
3. Minimizing the threat and risk of injury to law enforcement and others responsible for public protection, safety, or health.
4. Minimizing the threat and risk of damage to real or personal property.
5. Protecting individual privacy, civil rights, civil liberties, and other protected interests.
6. Protecting the integrity of criminal investigations, criminal intelligence, and justice system processes and information.
7. Minimizing reluctance of individuals or groups to use or cooperate with the justice system.

8. Supporting the role of the justice system in society.

9. Promoting governmental legitimacy and accountability.

10. Not unduly burdening the ongoing business of the justice system.

11. Making the most effective use of public resources allocated to public safety agencies.

C. Policy Applicability and Legal Compliance

1. All OIFC personnel, Oklahoma State Bureau of Investigation (OSBI) personnel who provide information technology services to the OIFC, and private contractors with direct access to OIFC information, will comply with the OIFC's privacy policy concerning the information the OIFC collects, receives, maintains, archives, accesses, or discloses to OIFC personnel, governmental agencies, including the eGuardian Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) SAR Data Repository (SDR).

2. The OIFC will provide a printed copy of this policy to all personnel who are assigned to the OIFC and have direct access to OIFC information and will require both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and the provisions it contains.

3. All OIFC personnel with direct access to OIFC information, OSBI personnel and private contractors with access to OIFC information and who provide information technology services to the OIFC shall comply with applicable laws protecting privacy, civil rights, and civil liberties.

4. The OIFC's internal operating policies are in compliance with applicable laws protecting privacy, civil rights, and civil liberties.

5. The OIFC's authority for the collection, use, analysis, and retention/destruction of intelligence and non intelligence information are cited in applicable constitutional provisions, 28 Code of Federal Regulations (CFR) Part 23 and in the following Oklahoma Statutes, Title 51 O.S., 24A.8, Title 74 O.S 150.5 (D), 74 O.S. 150.7 (2), 74 O.S. 150.9, 74 O.S. 150.12 and 74 O.S. 150.21a.

D. Governance and Oversight

1. As a result of Executive Order 2007-41, the Oklahoma Office of Homeland Security was directed to create a Governance Board for Oklahoma's Fusion Center to provide strategic direction, ensure objectives are achieved, risks are managed appropriately, and resources are used responsibly. A Steering Committee representing significant participants in the OIFC was also established, and meets regularly to provide input due to the collaborative nature of the

OIFC. Primary responsibility for the operation of the OIFC, its' justice systems, operations, and 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 OIFC

2. The Governance Board directed the OIFC to develop a Privacy Policy. The Governance Board and Steering Committee ensures that privacy and civil rights are protected within the provisions of this policy and within the OIFC's information collection, retention, and dissemination processes and procedures. The Governance Board has mandated that the policy be reviewed and updated as appropriate.

3. The OIFC has a trained Privacy Officer who receives reports regarding alleged errors and violations of the provisions of this policy. The Privacy Officer will serve as the liaison for the NSI eGuardian SDR.

4. The Privacy Officer is responsible for the direct oversight of the privacy policy regarding the collection, use, retention, destruction, sharing, classification, or disclosure of information and thus is responsible for notifying the Director of the OIFC regarding noncompliance issues.

E. Definitions

1. Primary terms and definitions used in the OIFC Privacy Policy are located in Appendix A., page 17.

F. Information

1. The OIFC's Watch Center serves as the focal point for the receipt of, and dissemination of, criminal and terrorism activity information. The receipt and dissemination of information is recorded and maintained in the Watch Center's Call Log Information Sheet. All information sought and collected is noted in the Watch Center's Call Log Information Sheet. OIFC's information is received from and disseminated to local, state, federal and tribal law enforcement, other Fusion Centers, the public, and to private entities as appropriate. The Watch Center also supports emergency operations centers which coordinate Oklahoma's response to significant man-made and natural disaster incidents.

2. The OIFC will seek, view and/or retain information that:

   a. Is based on a criminal predicate or threat to public safety; or

   b. Is based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal (including terrorist) conduct or activity; or

c. Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders of sentences; or the prevention of crime; or

d. Is useful in crime analysis or in the administration of criminal justice and public safety (including topical searches); and

e. The source of the information is reliable and verifiable or limitations on the quality of the information are identified; and

f. The information was collected in a fair and lawful manner, with the knowledge and consent of the individual, if appropriate.

3. All OIFC information will be sought, retained, shared, or disclosed under the appropriate policy provisions.

4. The OIFC may retain information that is based on a level of suspicion that is less than reasonable suspicion such as tips and leads or suspicious activity report information, subject to the policies and procedures issued. Suspicious Activity Reports (SAR) information will be provided to eGuardian, the Federal Bureau of Investigation's SAR database. Tips and leads and SAR information will be labeled separately from other information.

5. The OIFC 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 noncriminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, or sexual orientations.

6. The OIFC personnel will, upon receipt of information, evaluate the information to determine its nature, usability, and quality. Personnel will assign labels to the information to reflect the assessment, and to ensure the proper segregation of information, as appropriate, such as;

a. Whether the information is based upon a standard of reasonable suspicion of criminal activity;

b. Whether reported suspicious activity consists of observable behaviors which are consistent with established SAR guidelines as possible pre-operational planning for a criminal or terrorism event;

c. Whether the information consists of tips and leads data or suspicious activity reports;

d. The nature of the source as it affects veracity (for example, anonymous tips, trained interviewer or investigator, public record, private sector); and

e. The validity of the content (for example, verified, partially verified, unverified, or unable to verify).

7. At the time a decision is made to retain information, it will be labeled pursuant to applicable limitations on access and sensitivity of disclosure to:

   a. Protect confidential sources and law enforcement undercover techniques and methods;

   b. Not interfere with or compromise pending criminal or terrorism investigations;

   c. Protect an individual's right of privacy, civil rights, and civil liberties; and

   d. Provide legally required protection based on the individual's status such as a juvenile.

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

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

   b. There is a change in the use of the information affecting access or disclosure limitations; for example, the information becomes part of court proceedings for which there are different public access laws.

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

   a. Prior to allowing access to or dissemination of the information, ensure that attempts to validate or refute the information have taken place and that the information has been assessed for sensitivity and confidence by subjecting it to an evaluation or screening process to determine its credibility and value. The OIFC will use a standard reporting format for SAR information.

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

   c. Allow access to or disseminate the information using the same (or a more restrictive) access or dissemination standard that is used for data that rises to the level of reasonable suspicion (for example, —need-to-know and —right-to-know access or dissemination).

   d. Regularly provide access to or disseminate the information in response to an interagency inquiry for law enforcement, homeland security, or public safety and analytical purposes or

provide an assessment of the information to any agency, entity, individual, or the public when credible information indicates potential imminent danger to life or property.

e. Adhere to and follow the OIFC's physical, administrative, and technical security measures that are in place for the protection and security of tips and leads information. Tips, leads, and SAR information will be secured in a system that is the same or similar to the system that secures data that rises to the level of reasonable suspicion.

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

11. For purposes of sharing information, the OIFC will identify and label all terrorism related information per eGuardian policies and procedures, and provide the enhanced privacy protections for such information as are specified in this policy.

12. The OIFC will attach specific labels that will be used, assessed, or disseminated to clearly indicate any legal restrictions on information sharing based on information sensitivity or classification.

13. The OIFC will keep a record of the source of all information retained.

G. Acquiring and Receiving Information

1. Information gathering and investigative techniques used by the OIFC and participating agencies are in compliance with and will adhere to regulations and guidelines, including, but not limited to:

   a. 28 CFR Part 23 regarding criminal intelligence information.

   b. Organisation for Economic Co-operation and Development's *Fair Information Practices* (under certain circumstances, there may be exceptions to the *Fair Information Practices,* based, for example on authorities paralleling those provided in the federal Privacy Act; state, local and tribal laws; or OIFC policy.)

   c. Applicable criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) *National Criminal Intelligence Sharing Plan* (NCISP).

   d. Applicable constitutional provisions, State of Oklahoma Executive Order 2007-41 and Oklahoma Statutes which include Title 47 O.S. 2-129, Title 51 O.S., 24A.8, Title 51 O.S.

24A.28, Title 70 O.S. 3311 (E) (5), Title 74 O.S. 150.5 (D), 74 O.S. 150.7, 74 O.S. 150.9, 74 O.S. 150.12 and 74 O.S. 150.21a.

2. The OIFC'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 criminal or terrorism nexus. Law enforcement officers and OIFC personnel will be trained to recognize those behaviors and incidents that are indicative of criminal activity.

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

4. The OIFC utilizes eGuardian as its SAR database.

5. Information gathering and investigative techniques used by the OIFC will be the least intrusive means necessary in the particular circumstance to gather information it is authorized to seek or retain.

6. External agencies that receive and share information with the OIFC are governed by the laws and rules governing those individual agencies as well as by applicable federal and state laws.

7. The OIFC will contract only with commercial database entities that demonstrate that their methods for gathering personally identifiable information comply with applicable local, state, tribal, territorial, and federal laws, statutes, and regulations and that these methods are not based on misleading information collection practices.

8. The OIFC will not directly or indirectly receive, seek, accept, or retain information from:

   a. An individual or information provider that is legally prohibited from obtaining or disclosing the information.

H. Information Quality Assurance

1. The OIFC will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources of information. The OIFC will make every reasonable effort to ensure that the information is accurate, current and complete, including the relevant context in which it was sought or received; and the information is merged about the same individual or organization only after utilizing the applicable standards.

2. At the time of retention in the system, the information will be accessed and labeled regarding its level of quality (current, verifiable, and reliable).

3. The OIFC investigates, in a timely manner, alleged errors and deficiencies and corrects, deletes, or refrains 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 confidence (validity and reliability) in previously retained information.

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

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

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

I. Collation and Analysis

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

2. Information subject to collation and analysis is information as defined and identified in Section E, Information.

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

   a. Further crime prevention (including terrorism), law enforcement, force deployment, or prosecution objectives and priorities established by the OIFC, and

b. Provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in, or engaging in, criminal or terrorist activities.

J. Merging Records

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

2. 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.

3. 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. Access to OIFC information:

   a. The Director of the OIFC, and/or administrator(s) designated by the Director, shall establish requirements and record all personnel as to their access authority and permission to access OIFC's information;

   b. Permission's regarding viewing, adding, editing and printing of OIFC information is controlled by OIFC's administrator(s) on all OIFC's information;

   c. All OIFC personnel, with approval from the Director, or his designee, may disclose OIFC information pursuant to applicable policy;

   d. An audit trail shall be maintained regarding access to, and disclosure of, OIFC information.

2. The OIFC will adhere to national standards for the suspicious activity reporting (SAR) process, including the use of a standard reporting format and the FBI's eGuardian standards.

3. Access to, or disclosure of, records retained by the OIFC will be provided only to persons within the OIFC or in other governmental agencies who are authorized to have access, and only for legitimate law enforcement, public protection, public prosecution, public health, or justice purposes, and only for the performance of official duties in accordance with law and procedures applicable to the agency for which the person is working. The Watch Center Call Log Information Sheet records all disseminations of information by OIFC personnel. All disseminations with personally identifiable information (PII) are approved by the OIFC Director, Analytic Supervisor, and the Privacy Officer. Exceptions are when one of the approvers are not available. This approval process is documented on the cover sheet for all OIFC products. Products without PII are approved by the OIFC Director and Analytic Supervisor, but in most incidences the products are approved by all three approvers. Information regarding a previously issued product requiring a close out may be disseminated without further approval unless there is something unique about that product. Agencies external to the OIFC may not disseminate OIFC information received from OIFC without approval from the originator of the information.

4. Records retained by the OIFC may be accessed or disseminated to those responsible for public protection, public 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. As stated, the Watch Center Call Log Information Sheet records all disseminations.

5. Information gathered and records retained by the OIFC may be accessed or disseminated for specific purposes upon request by persons authorized by law to have such access, and only for those users and purposes specified in the law. The Watch Center Call Log Information Sheet which notes receipt and dissemination of this type of information will be kept a minimum of five years for this type of request. Thus requests and disseminations for specific purposes are recorded and maintained.

6. Information gathered and records retained by the OIFC may be accessed or disclosed to a member of the public only if the information is defined by law to be a public record pursuant to Oklahoma Statute, Title 51 O.S. 24A.8 or otherwise appropriate for release to further the OIFC 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 OIFC for this type of information or when there is a legitimate need. Requests of this nature are recorded in the Watch Center Call Log Information Sheet. The request and any information disclosed are recorded in the Watch Center Call Log Information Sheet.

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

    a. Sold, published, exchanged, or disclosed for commercial purposes;

    b. Disclosed or published without prior notice to the originating agency that such information is subject to re-disclosure or publication, unless disclosure is agreed to as part of the normal operations of the agency; or

c. Disseminated to persons not authorized to access or use the information.

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

   a. Records required to be kept confidential by law are exempted from disclosure requirements under Oklahoma Statute, Title 51 O.S. 24A. 5.

   b. Investigatory records of law enforcement agencies are exempted from disclosure requirements under Oklahoma Statutes, Title 51 O.S. 24A. 8 and Title 74 O.S. 150. 5 (D). However, certain law enforcement records must be made available for inspection and copying under Oklahoma Statute, Title 51 O.S. 24A. 8.

   c. A record, or part of a record, the public disclosure of which would have a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack is exempted from disclosure requirements under Oklahoma Statutes, Title 51 O.S. 24A. 27 and Title 51 O.S. 24A. 28. This includes a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism under Oklahoma Statutes, Title 51 O.S. 24A. 27 and Title 51 O.S. 24A. 28 or an act of agricultural terrorism under Oklahoma Statutes, Title 51 O.S. 24A. 27 and Title 51 O.S. 24A. 28, vulnerability assessments, risk planning documents, needs assessments, and threat assessments.

   d. Protected federal, state, local, or tribal records, which may include records originated and controlled by another agency that cannot be shared without permission.

   e. A violation of an authorized nondisclosure agreement.

9. The OIFC shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.

L. Redress

1. Disclosure

   a. Requests for disclosure of OIFC records by the public will be handled according to established procedures under Oklahoma's Open Records Act, Title 51 O.S. 24A.1 et seq. The OIFC's response to the request for information will be made within a reasonable time and in a form that is readily intelligible to the individual. A record will be kept of all requests and of what information is disclosed to an individual.

   b. The existence, content, and source of the information will not be made available to an individual when:

i. Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution (Title 51 O.S. 24.8 (C));

ii. Disclosure would endanger the health or safety of an individual, organization, or community (Title 51 O.S. 24.8 (C));

iii. The information is in a criminal intelligence system (Title 74 O.S. 150.21 (a));

iv. Disclosure to the individual is exempt or prohibited by applicable U.S. Code, state statute or administrative rule;

v. The information source does not reside with the OIFC (Title 51 O.S. 24.8 (C)); or

vi. The OIFC did not originate or does not have a right to disclose the information (Title 51 O.S. 24.8 (C)).

2. Complaints and Corrections

a. If an individual has complaints or objections to the accuracy or completeness of information about him or her originating from OIFC information, the OIFC will inform the individual of the procedure for submitting complaints or objections (if not properly communicated) or requesting corrections. If an individual's complaint or objection cannot be resolved after review at the OIFC, the individual may request a review of that decision, by the Director of the OSBI, as the OSBI is the host agency for the OIFC. A record will be kept of all complaints and requests for corrections and the resulting action, if any.

b. If an individual has complaints or objections to the accuracy or completeness of information about him or her that originates with another agency, the OIFC will notify the source agency of the complaint or request for correction, and coordinate with the source agency to ensure that the individual is provided with applicable complaint submission or corrections procedures. A record will be kept of all such complaints and request for corrections, and the resulting action taken, if any.

c. The individual to whom information has been disclosed will be given reasons if requests for correction(s) are denied by the OIFC, or the originating agency.

3. Redress

a. If an individual has complaints or objections to the accuracy or completeness of OIFC/SAR information allegedly held by the OIFC that has resulted in specific, demonstrable harm to such individual, the OIFC will inform the individual of the procedure for submitting complaints or requesting corrections (if not properly communicated). The OIFC will acknowledge the complaint and state that it will be reviewed, but will not confirm the existence of any OIFC/SAR information in privacy fields that identifies the individual. However, any personal

information will be reviewed and corrected in, or deleted from, OIFC/SAR shared space if the information is determined to be erroneous, included incorrectly merged information, or is out of date. A record will be kept of all complaints and requests for corrections, and the resulting actions, if any.

M. Security Safeguards

1. The OIFC's Fusion Center has a designated and trained Security Officer.

2. The OIFC is located within the headquarters of the OSBI, which is a secure facility, thus protected from external intrusion. The OIFC's office space is only accessible to OIFC personnel and other OSBI personnel that have been issued an access card for the OIFC. The OIFC will utilize secure internal and external safeguards against network intrusions. Access to OIFC systems from outside the facility will be allowed only over secure networks. The OIFC's information system is an OSBI system and thus maintained by them. All OSBI systems, to include the OIFC system, are required to complete an annual security risk assessment as a result of Oklahoma Statute Title 62 O.S. 41.5a (A) (13). The purpose of this annual assessment is to identify vulnerabilities. All OSBI information systems are required to be compliant with ISO/IE 17799 standards, National Institute of Standards and Technology Special Publications 800-30 standards, and PCI DSS standards.

3. The OIFC will initially process tips, leads, and SAR information in a SAR vetting tool. Ultimately, this information will be appropriately labeled and incorporated into eGuardian, a repository system that is the same as, or similar to, the system that secures data rising to the level of reasonable suspicion.

4. The OIFC 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.

5. Direct access to OIFC's information will be granted only to OIFC 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.

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

7. The OIFC utilizes' the Watch Center Call Log Information Sheet to record requested and disseminated information.

8. To prevent public records disclosure, risk and vulnerability assessments are stored in the Automated Critical Asset Management System database, a separate system, and will not be stored with publicly available data.

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

N. Information Retention and Destruction

1. All OIFC generated information (intelligence/non-intelligence) and/or information (intelligence/non-intelligence) furnished to OIFC, some of which may be for dissemination, will be reviewed for record retention (validation or purge) at least every five years.

2. Procedures for handling non-intelligence information regarding retention and destruction is stated in Oklahoma Statutes, Title 51 O.S., 24A.8, Title 74 O.S. 150.5 (D), 74 O.S. 150.7 (2), 74 O.S. 150.9 and 74 O.S. 150.12.

3. The Oklahoma Statewide Intelligence Network Guidelines will be followed regarding the retention and destruction of OIFC intelligence information. The present guidelines are located in Appendix B, page 27.

4. The OIFC will delete information, or return it to the source, as required in Oklahoma Statutes, or as specified in 28 CFR Part 23.

5. The retention and destruction of SAR's information is governed by the FBI's retention and destruction policy, as OIFC's SARs are inputted in eGuardian.

6. All OIFC information will be periodically reviewed for relevancy and importance. Information which has been determined to be invalid, untrue, obsolete, no longer useful because the purpose for which it was collected has been satisfied or no longer exists will be purged, destroyed, and deleted from the system. The OIFC is not required by law or regulation to notify source agencies of the purge of information or intelligence from OIFC databases. Source agencies will not be notified when information they have submitted is due for purge from OIFC information or intelligence databases. Purged dates will be tracked in electronic databases based on the date of record entry into the database.

O. Accountability and Enforcement

1. Information System Transparency

   a. The OIFC will be open with the public in regard to information and intelligence collection practices. The OIFC's Privacy Policy will be provided to the public upon request.

b. The OIFC's Privacy Officer will be responsible for receiving inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s). The OIFC's Privacy Officer will report all inquiries and complaints to OSBI's Legal Department. The Legal Department will direct the handling and response to inquiries/complaints.

2. Accountability

a. The Watch Center Call Log Information Sheet records queries, disseminations and other pertinent information. Accessing the Watch Center Call Log Information Sheet identifies the user in the OIFC's audit system.

b. The OIFC, through entries in the Watch Center Call Log Information Sheet, maintains information of accessed, requested, or disseminated information. The Watch Center Call Log Information Sheet will be kept for five years to identify who requested information and to whom information was disseminated. The OIFC's audit system records access to the Watch Center Call Log Information Sheet.

c. The OIFC will provide a copy of this policy to all OIFC personnel and will require written acknowledgement of receipt of this policy and the provisions it contains.

d. The OIFC's Privacy Officer will periodically conduct audits to ensure and evaluate the compliance of users.

e. The OIFC's personnel, or other personnel participating with the OIFC, shall report violations or suspected violations of OIFC policies relating to protected information to the OIFC's Privacy Officer and/or the Director.

f. The Privacy Officer will conduct an annual audit and inspection of the Watch Center's information.

g. The OIFC's Governance Board and Steering Committee, guided by the trained Privacy Officer, will review and update the provisions protecting privacy, civil rights, and civil liberties contained within this policy at least annually and will make appropriate changes in response to changes in applicable law, technology, the purpose and use of the information systems, and public expectations.

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

3. Enforcement

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

      i. Notify in writing the chief executive of the employing agency of the violation and noncompliance of his or her employee.

      ii. Initiate an investigation, criminal if appropriate.

      iii. As the OIFC is a multi-agency effort, OIFC's Director will work with each agency regarding their personnel policies for appropriate sanctions that do not rise to the criminal matter.

      iv. Agencies must take action to correct such violations and provide an assurance in writing to the OIFC Director that corrective action has been taken.

      v. The failure to remedy violations may result in suspension or termination of access by the employee to OIFC information.

      vi. The OIFC reserves the right to restrict the qualifications and number of personnel having direct access to OIFC information, and to suspend or withhold service to any participating agency user who fails to comply with the applicable restrictions and limitations of the OIFC's Privacy Policy.

P. Training

1. The OIFC will require annual training for the following individuals regarding implementation of and adherence to the Privacy Policy:

   a. Any person that is granted direct access to OIFC information

2. The OIFC provides training to personnel authorized to share protected information through the eGuardian NSI SDR.

3. The OIFC's Privacy Policy training program will cover:

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

   a. Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the OIFC;

b. How to implement the policy in the day-to-day work of the user, whether a paper or systems user;

c. The impact of improper activities associated with infractions within or through the agency;

d. Mechanisms for reporting violations of OIFC privacy-protection policies; and

e. The nature and possible penalties for policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.

Appendix A – Definitions

The following are the primary terms and definitions used in this privacy policy document:

Access – Data access is being able to get to (usually having permission to use) particular data on a computer. Web access means having a connection to the World Wide Web through an access provider or an online service provider. Data access is usually specified as read-only and read/write access.
With regard to the eGuardian NSI SDR, access refers to the business rules, means, and processes by and through which eGuardian NSI SDR participants obtain terrorism-related information, to include homeland security information, terrorism information, and law enforcement information acquired in the first instance by another eGuardian NSI SDR 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 eGuardian NSI SDR 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 eGuardian NSI SDR participants through, for example, news reports or to the obtaining of information shared with them by another eGuardian NSI SDR participant who originally acquired the information.

Agency – Agency refers to the (name of agency) and all agencies that access, contribute, and share information in the (name of agency)'s justice information system.

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. They 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.)

Authorized User – A person that is granted direct access to OIFC information.

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.

Call Log Information Sheet – The input form used by OIFC personnel in the OIFC Watch Center to record information received and disseminated.

Civil Rights – The term "civil rights" is used to imply that the state has a role in ensuring that all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of race, religion, gender, or other characteristics unrelated to the worth of the individual. Civil rights are, therefore, obligations imposed on government to promote equality. More specifically, they are the rights to personal liberty guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments, and by acts of Congress.

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.

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

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

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

Criminal Intelligence Information or Data – Information deemed relevant to the identification of, and the criminal activity engaged in, by an individual 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.

Data – Insert symbols, signs, descriptions, 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, sharing, publication, or divulging of personal information in any manner – electronic, verbal, or in writing – to an individual, agency, or organization outside the agency that collected it. Disclosure is an aspect of privacy, focusing on information which may be available only to certain people for certain purposes but which is not available to everyone.

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 disc 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, or transmission over the Internet, intranet, extranet, leased lines, dial-up lines, private networks, telephone voice response, or faxback systems. It does not include faxes, telephone calls, video teleconferencing, or messages left on voicemail.

Fair Information Practices – The Fair Information Practices (FIPs) are contained within the Organisation for Economic Co-operation and Development's Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data. These were developed around commercial transactions and the trans-border exchange of information; however, they do provide a straightforward description of underlying privacy and information exchange principles and provide a simple framework for the legal analysis that needs to be done with regard to privacy in integrated justice systems. Some of the individual principles may not apply in all instances of an integrated justice system.
The eight FIPs are:

1. Collection Limitation Principle
2. Data Quality Principle
3. Purpose Specification Principle
4. Use Limitation Principle
5. Security Safeguards Principle
6. Openness Principle
7. Individual Participation Principle
8. Accountability Principle

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

Homeland Security Information – As defined in Section 892(f)(1) of the Homeland Security Act of 2002 and codified at 6 U.S.C. § 482 (f)(1), homeland security information means any information possessed by a federal, state, or local agency that (a) relates to a threat of terrorist activity; (b) relates to the ability to prevent, interdict, or disrupt terrorist activity; (c) would improve the identification or investigation of a suspected terrorist or terrorist organization; or (d) would improve the response to a terrorist act.

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

Individual Responsibility – Since a privacy policy is not self-implementing, an individual within an organization's structure must also be assigned responsibility for enacting and implementing the policy.

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

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

Invasion of Privacy – Invasion of privacy can be defined as 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 by this policy, law includes any local, state, or federal statute, ordinance, regulation, executive order, policy, or court rule, decision, or order as construed by appropriate local, state, or federal officials or agencies.

Law Enforcement Information – For purposes of the eGuardian NSI SDR, law enforcement information means any information obtained by, or of interest to, a law enforcement agency or official that is both (a) related to terrorism or the security of our homeland and (b) relevant to a law enforcement mission, including but not limited to information pertaining to an actual or potential criminal, civil, or administrative investigation, or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of, or response to, criminal threats and vulnerabilities; the existence, organization, capabilities, plans,

intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of or response to criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance.

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 privileges needed to accomplish the tasks he or she is authorized to perform.

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 data. (See also Audit Trail.)

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

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

Non-repudiation – A technique used to ensure that someone performing an action on a computer cannot falsely deny that he or she 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.

OIFC Watch Center – The location within OSBI headquarters where information is received, assessed, disseminated and retained.

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

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

- Personal characteristics (such as height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, 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 United States citizens, aliens known by the intelligence agency concerned to be permanent resident aliens, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. For the intelligence community and for domestic law enforcement agencies, "persons" means United States citizens and lawful permanent residents.

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

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

Privacy Protection – This is a process of maximizing the protection of privacy, civil rights, and civil liberties when collecting and sharing information in the process of protecting public safety and public health.

Protected Information – For the non-intelligence community, protected information is information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and laws of the United States. For state, local, and tribal governments, it includes applicable state and tribal constitutions and state, local, and tribal laws, ordinances, and codes. For the (federal) intelligence community, protected information includes information about "United States persons" as defined in Executive Order 12333. Protected information may also include other information that the U.S. government expressly determines by Executive Order, international agreement, or other similar instrument should be covered.

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; and
- 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; and
- Public agencies whose authority to access information gathered and retained by the agency/center is specified in law.

Public Access – Public access relates to what information can be seen by the public; that is, information whose availability is not subject to privacy interests or rights.

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

Redress – Internal procedures to address complaints from persons regarding protected information about them that is under the agency's/center's control.

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

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 – Security refers to the range of administrative, technical, and physical business practices and mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes. Computer and communications security efforts also have the goal of ensuring the accuracy and timely availability of data for the legitimate user set, as well as promoting failure resistance in the electronic systems overall.

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 eGuardian NSI SDR, 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 – Suspicious activity is defined as "reported or observed activity and/or behavior that, based on an officer's training and experience, is believed to be indicative of intelligence gathering or

preoperational planning related to terrorism, criminal, or other illicit intention". Examples of suspicious activity include surveillance, photography of facilities, site breach or physical intrusion, cyber attacks, testing of security, etc.

Suspicious Activity Reports – The observation and documentation of a suspicious activity. At the federal level, there are two types of SARs: 1) eGuardian NSI SDR SARs that pertain to terrorism information; and 2) Banking Secrecy Acts SARs that pertain to suspicious banking activity and is required to be completed by financial institutions. Suspicious activity reports offer a standardized means for feeding information repositories or data analysis tools. Patterns identified during SAR data analysis may be investigated in coordination with the reporting agency and, if applicable, the state-designated fusion center. SARs are not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor are they designed to support interagency calls for service.

Terrorism Information – In accordance with Intelligence Reform and Terrorism Prevention Act, as recently amended by the 9/11 Commission Act enacted on August 3, 2007 (P.L. 110-53), the Information Sharing Environment facilitates the sharing of terrorism, including weapons of mass destruction information, 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 Information Sharing Environment 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.

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. Tips and leads information is 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 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 falls between being of no use to law enforcement and being extremely valuable depending on the availability of time and resources to determine its meaning.

Appendix B – OKLAHOMA STATEWIDE INTELLIGENCE NETWORK GUIDELINES

Oklahoma Statewide Intelligence Network Guidelines

Mission Statement:
The mission of the Oklahoma Statewide Intelligence Network is to collect, analyze, disseminate, and manage information concerning the activity and identity of individuals or organizations reasonably believed to be engaged in criminal activity, and to provide assistance to investigators. The OSBI Criminal Intelligence Office will support the Statewide Intelligence Network by providing a clearinghouse of crime related information needed to coordinate the efforts of local, state, and federal agencies, and by providing training to law enforcement agency employees concerning the legal collection, preservation, and dissemination of crime related information.

Definitions

28 CFR Part 23 – Section 28 Part 23 of the Code of Federal Regulations. This code governs Criminal Intelligence Offices which receive federal funding to operate.

Analysis – The function of handling, sorting, and filing information, including the sifting out of useless information, the orderly arrangement of collected materials so relationships can be established, and the creation of a system for rapid retrieval of filed information.

Assessment – An estimate, evaluation, or appraisal of information content and its possible impact.

Classification – A rating given stored information. A classification indicates access and dissemination restrictions.

Collation – Assembling in proper order to clarify or give meaning to information.

Crime Prevention – A proactive step taken by law enforcement officers and prosecutorial authorities that anticipates, hinders, frustrates, or stops suspected criminal activity. Crime prevention does not include dissemination of information to persons other than commissioned peace officers.

Criminal Intelligence Office – The arrangements, equipment, facilities, and procedures used for the receipt, storage, dissemination, and analysis of criminal intelligence information.

Dissemination – The transmission of intelligence orally, in writing, electronically, or by any other means, from the person having custody of the intelligence to another person.

Information – Written or oral reports or documents telling of an event or activity. Information may take the form of fact, opinion, rumor, or inference.

Intelligence – Information that has been processed (i.e., collected, evaluated, collated, analyzed, and reported).

Need to Know – The requested intelligence is pertinent and necessary to the requester's criminal investigation. A direct official involvement in an investigation or a reason for requesting the information must exist.

Raw Data – Information that has not been put through the intelligence process.

Right to Know – The requester has the official capacity and the legal authority under Title 74 O.S. § 150.21(a) or the OSBI Administrative rules, to the intelligence information being requested.

Statewide Intelligence Network – The Statewide Intelligence Network was developed to provide a secure and comprehensive intelligence and investigative tool for local law enforcement throughout the State of Oklahoma. Participating users of the Statewide Intelligence Network will have access to a centralized program designed to encourage communication and information sharing among law officers in the enduring effort to serve and protect the communities of our State. The Oklahoma State Bureau of Investigation will house and maintain the Statewide Intelligence Network.

Source Document – The original document in file. This will normally be a hard copy of the intelligence information entered into the Statewide Intelligence Network. The source document must be maintained by the originating agency.

General Guidelines

All information collected and entered into the Statewide Intelligence Network MUST be based upon a standard of reasonable suspicion of criminal activity, and the information submitted must be relevant to that activity. Reasonable suspicion of criminal activity is defined here as:

A level of certainty created in the mind of an experienced and trained police officer in which there is a reasonable possibility an individual or organization is involved in a definable criminal activity or enterprise.

The OSBI's Criminal Intelligence Office and all authorized Statewide Intelligence Network users shall not collect, maintain, or disseminate information which is solely and exclusively about an individual's sexual, political or religious activities, beliefs, or opinions, unless the information is crime related.

The OSBI's Criminal Intelligence Office and all authorized Statewide Intelligence Network users will not solicit nor will they use information obtained by illegal or unauthorized methods. No information obtained in violation of any applicable Oklahoma or Federal law shall be submitted to, accepted by, stored, or distributed by the Statewide Intelligence Network.

Authorized Statewide Intelligence Network users shall exercise all due caution and discretion in the use of information collected, maintained, and disseminated so as not to violate the Constitutional rights of any person.

Any violation of these guidelines could cause revocation of access to the Statewide Intelligence Network.

Information Collection

Information for submission to the Statewide Intelligence Network can be collected from a variety of sources, including, but not limited to: informants, print and electronic media, public records, subpoenaed documents, and undercover operations. Collection will always be based upon reasonable suspicion of criminal activity, and will be conducted by lawful methods.

Information Submission

All information submitted to the Statewide Intelligence Network should be maintained by the submitter in report form.

If the information meets the standards set forth in these guidelines, the information may be entered into the Statewide Intelligence Network. Each file will be assigned a unique, computer generated file number.

The Statewide Intelligence Network is a system which allows each intelligence report to be linked to other intelligence that has been submitted. Each report can be linked to any other REPORT, SUBJECT, GROUP, or BUSINESS. As each new report is entered into the system, names should be checked against reports already in the system so information will not be duplicated. This also allows for the notification of the submitter if someone other than themselves has submitted intelligence on a particular subject or group. For entry into the Statewide Intelligence Network the following information is required:

Intelligence Classification: The Statewide Intelligence Network requires a classification be assigned to the intelligence. The classifications are as follows:

Confidential: This information is considered by the user to be intelligence information that might be useful to other law enforcement agencies, and may be viewed by all authorized Statewide Intelligence Network users.

Sensitive/Classified: If an authorized Statewide Intelligence Network user searches for information currently in the network as Sensitive/Classified information, a message will be displayed to contact the creator or the creator's agency for the information. The creator or submitter must make the determination as to the requester's "Right to Know" or "Need to Know" the information.

Secret: If an authorized Statewide Intelligence Network user searches for information currently in the network as Secret information, a message will be displayed to contact the OSBI. The OSBI will contact the submitter for authorization to release the information. The identification of the submitter will not be revealed without the permission of the submitter.

Restrictions: An additional restriction will be available to submitters:

Law enforcement – may be viewed by all authorized Statewide Intelligence Network users.

Internal – may only be viewed by the creator or the creator's agency.

Draft – entry of intelligence information is still in progress. Only the creator or the creator's agency will be able to view this information until the entry is completed and the restriction level is changed to the appropriate level.

Classification	*Restriction*	*Viewing Authorization*
Confidential	Law Enforcement	All authorized SIN users
Confidential	Internal	Creator; Creator's agency; Other agency users will be told to contact creator or creator's agency
Confidential	Draft	Creator; Creator's agency; Other agency users will be told record is not ready for distribution & to contact creator or creator's agency.
Sensitive/Classified	Law Enforcement	Creator; Creator's agency; Other agency users will be told to contact creator or creator's agency.
Sensitive/Classified	Internal	Creator; Creator's agency; Other agency users will be told to contact creator or creator's agency.
Sensitive/Classified	Draft	Creator; Creator's agency; Other users will be told record is not ready for distribution & to contact creator or creator's agency.
Secret	Law Enforcement	Creator; Creator's agency; Other agency users will be told to contact OSBI.
Secret	Internal	Creator; Creator's agency; Other agency users will be told to contact creator or creator's agency.
Secret	Draft	Creator; Creator's agency; Other agency users will be told record is not ready for distribution & to contact creator or creator's agency.

Source of Information: This is the individual who provided the intelligence. In some cases, the submitter may also be the source of the information.

Use of Confidential Informant(s)

In the case of a confidential informant, a number would be used in place of the informant's name. If the source is a confidential informant, it is the responsibility of the user to maintain documentation pertaining to the identity of the confidential informant.

Note: Authorized Statewide Intelligence Network agencies will be provided a code to be used when assigning confidential informant numbers to prevent entry of the same number by multiple agencies.

1. The source **reliability** will be classified by the submitter as:

    a. Reliable;
    b. Unreliable;
    c. Usually reliable;
    d. Unknown;

2. The submitter will also identify the source **type** as:

    a. Criminal Source – An individual whose lifestyle, either through criminal record or association, is characteristic of criminal activity;
    b. Informant – Confidential source identified on the Confidential Informant Form;
    c. Law Enforcement – a law enforcement officer;
    d. Other (i.e., citizens, public documents, media, etc.)

3. The user will assess the **content** validity as:

    a. Verified;
    b. Partially verified;
    c. Unverified;
    d. Unable to verify.

Inquiry Procedure

I. An inquiry for information from the Statewide Intelligence Network may come from other local, state, or federal law enforcement agencies and/or prosecutorial authorities for the purpose of criminal investigation, criminal prosecution, and crime prevention. These inquiries may be received either orally, written, or electronically.

II. The authorized Statewide Intelligence Network user will first establish the requester's "Need to Know" or "Right to Know" the information.

III. Audit capabilities incorporated into the Statewide Intelligence Network allow for the ability to identify which user has accessed specific intelligence in the network, even if the user only viewed the information. The OSBI's Criminal Intelligence Office strongly recommends each user keep a log of searches which resulted in a positive response. If questioned why the user accessed the specific intelligence, the user will be able to reference this log and determine why the search/viewing was performed.

Dissemination, Viewing, Printing, and Use of Information

I. Information developed as a result of an inquiry may be disseminated only in accordance with the established security guidelines, security levels, and statutes. Information contained in the Statewide Intelligence Network will not be disseminated, either orally or in writing, formally or informally, to any non-law enforcement agency or individual, except as legally authorized. Title 74 O.S. § 150.21(a) prohibits the release of information to anyone other than law enforcement officers and prosecutorial authorities, for the purpose of criminal investigation, criminal prosecution, and crime prevention.

   Unauthorized release or use of intelligence information is a misdemeanor and can result in incarceration and/or a $50,000 fine. Strict controls shall be maintained in the dissemination of information from the Statewide Intelligence Network. However, dissemination of an assessment of criminal intelligence information may be made to normally unauthorized individuals when necessary to avoid imminent danger to life or property. It is the responsibility of the individual disseminating the information to make certain the request for data is for a legitimate law enforcement purpose.

II. Prior to the dissemination of any intelligence, the following shall be considered:

   A. The requester's right and need to know.
   B. The accuracy and reliability of the intelligence.
   C. Whether the dissemination of the intelligence would compromise an investigation or the identity of a confidential source of information.

III. The Statewide Intelligence Network requires an entry to the dissemination log each time a printed copy is requested. This entry will show the type of request, who received the information, and what agency they represent.

Storage of Intelligence Information

I. Intelligence source documents should be independent and isolated from all other department files. All criminal intelligence data should be kept in a locked and secure area. There are two basic types of intelligence information to be stored:

A. **Computerized Information.** Information which has met the established criteria will be stored in the Statewide Intelligence Network. Access to this software will be strictly controlled by password and the data collected will be partitioned by assigning security levels of access.

B. **Non-computerized Information.** Information which is acceptable but cannot be computerized will be marked and identified, and placed in a secure storage area. It will be linked to the appropriate intelligence in the computer database and will be subject to the same level and dissemination as other information. This type of information could include video or audio recordings, for example. Once these items are marked and identified, they should be stored in a secure area.

II. Intelligence files should be protected by physical and procedural safeguards which prohibit entry by other than authorized personnel.

III. All confidential criminal intelligence information will be kept locked and secure during other than normal working hours.

IV. All file cabinets and desks which are not kept in locked quarters and contain criminal intelligence files will be locked when not in direct use by authorized personnel.

Review, Retention and Purging of Information

I. All information stored in the Statewide Intelligence Network must be periodically reviewed for relevancy and importance. A review of the system by Criminal Intelligence Office personnel will take place periodically. The submitter of information which has become misleading, obsolete, or otherwise unreliable will be notified data should be destroyed and/or purged from the system.

II. The objective of the intelligence system purging policy is to totally eliminate intelligence from the system when any one of the following conditions apply:

A. The intelligence is no longer useful because the purpose for which it was collected has been satisfied or no longer exists.

B. The intelligence is obsolete because its age makes it unreliable for present purposes.

C. The intelligence has been found to be invalid, untrue, or misleading.

D. All information on the subject in file has been ordered sealed or destroyed by competent judicial authority. A certified copy of the court order should be placed in the file with the original source document containing the affected information. The court ordered restrictions will be immediately complied with upon being notified of the court order, although no destruction will be done until a certified copy of the order is received.

The OSBI's Criminal Intelligence Office **MUST** notified immediately upon receipt of such order so information can be removed from the Statewide Intelligence Network.

III. The decision to purge or retain intelligence data contained in the Statewide Intelligence Network will be based upon, but not limited to, the following considerations:

A. **The age of the intelligence information.** When was the intelligence first entered into the system, and does the date of the offense involved fall within the statute of limitations, or is the nature of the information time sensitive?

B. **Frequency of use.** How often has the intelligence been used since it was entered into the system?

C. **Initial reason for collection.** Does the purpose for which the intelligence was collected still exist?

D. **Nature of the information.** How important, significant, or sensitive is the information?

E. **Quality and reliability.** Is the information a confirmed fact, hypothesis, opinion, or unsubstantiated rumor?

F. **Completeness and accuracy.** When was the information last updated and what effort is required to validate or update it now?

G. **Usefulness.** What is the information's present and potential utility?

H. **Impact on law enforcement.** What effect would purging the information from the intelligence files have on the law enforcement community?

I. **Availability.** Can the information be obtained from other sources?

IV. Periodically, the OSBI's Criminal Intelligence Office will query the Statewide Intelligence Network to determine which reports are due for purge. The submitter of the intelligence will be contacted electronically and asked to update the information. If the intelligence can be updated, the report

may remain in the system, and a new retention date established. If it is not updated, and no articulated reason is found for retention, the report will be purged from the intelligence system.

V. Purging consists of the removal of the intelligence report from the Statewide Intelligence Network and its physical destruction. All computerized records of the intelligence report and its data shall be permanently erased from the computerized intelligence system database so the information cannot be retrieved.

VI. The intelligence data that is purged will be totally eliminated from the system. Nothing should remain in a file that has been purged, which once identified a person or organization. Only the assigned file number will remain in the computer system for continuity and audit purposes.

Destruction of Purged Material

I. Purged documents and materials will be destroyed either by a supervised burning or shredding process, or by some other method which will totally destroy the material.