
# OCTIC Privacy Policy

# Table of Contents

OKLAHOMA COUNTER TERRORISM INTELLIGENCE CENTER
Oklahoma's Fusion Center

# OCTIC Privacy Policy

The Oklahoma Counter Terrorism Intelligence Center (hereinafter "OCTIC" or "the center") is Oklahoma's statewide fusion center. OCTIC was created in 2008 (Executive Order 2007-41). In 2023, the Oklahoma Department of Public Safety was charged with management of OCTIC's daily operations (Executive Order 2022-31). Pursuant to Executive Order 2023-07, Oklahoma's fusion center was given the name OCTIC.

OCTIC was formed to foster and facilitate the sharing of information among Oklahoma's law enforcement agencies and public safety agencies and to further empower those agencies to protect the citizens of Oklahoma. OCTIC serves as the focal point for the collection, assessment, analysis, and dissemination of terrorism intelligence and information concerning other criminal activity that may impact Oklahoma (Executive Order 2022-31).

OCTIC's mission is to protect the residents, visitors, communities, schools, and critical infrastructure in Oklahoma through enhanced counterterrorism, criminal intelligence, investigative, and cyber security support in collaboration with local, state, tribal, federal, and private partners.

## I. Policy Purpose

The purpose of this privacy, civil rights, and civil liberties (P/CRCL) policy is to promote conduct by OCTIC and its participating agencies that complies with applicable federal, state, and local laws; guide OCTIC in compliance with 28 C.F.R. Part 23; and assist OCTIC and its participating agencies in:

- Increasing public safety and promoting homeland security;
- Minimizing the threat and risk of harm to specific individuals;
- Minimizing the threat and risk of harm to law enforcement and others responsible for public protection, safety, or health;
- Minimizing the threat and risk of damage to real or personal property;
- Protecting individual privacy, civil rights, civil liberties, and other protected interests;
- Protecting the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information;
- Encouraging individuals and community groups to trust and cooperate with the justice system;
- Supporting the role of the justice system in society;
- Promoting governmental legitimacy and accountability; and
- Making the most effective use of public resources allocated to public safety agencies.

This policy is intended solely to guide OCTIC in the performance of its functions, and this policy shall not be construed to create or confer on any other person or entity any right or benefit, substantive or procedural, enforceable at law or otherwise against OCTIC, the Department of Public Safety, or other sponsor under whose auspices a party is participating in OCTIC, or the officers, directors, employees, detailees, agents, representatives, task force members, contractors, subcontractors, consultants, advisors, successors, assignees or other agencies thereof. The provisions of this policy shall not be enforceable by any third party.

## II. Policy Applicability and Legal Compliance

All OCTIC personnel, participating agency personnel, personnel providing information technology services to the center, private contractors providing services to the center, and other authorized users who are not employed by the center or a contractor shall comply with this policy. This policy applies to information the center gathers or collects, receives, maintains, stores, accesses, discloses, or disseminates to governmental agencies, personnel of governmental agencies, private contractors, private entities, and the general public.

OCTIC will provide a printed or electronic copy of this policy to personnel employed by, or detailed to, OCTIC, participating agencies and individual users, and non-center personnel who provide services to the center with unescorted access to the center or its intelligence system(s). OCTIC will require both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and the applicable provisions it contains (Appendix A).

## III. Governance and Oversight

Primary responsibility for the operation of OCTIC; its systems, operations, and coordination of personnel; the receiving, seeking, retention, evaluation, data quality, analysis, destruction, sharing, disclosure, or dissemination of information; and enforcement of this policy is assigned to the OCTIC Director, as appointed by the Oklahoma Commissioner of Public Safety.

The OCTIC Governance Board is responsible for establishing policy for the operation of the center and may make recommendations pertaining to processes and procedures established by the center in fulfillment of its mission. The Governance Board may also provide guidance regarding budget and manpower issues and provide guidance as to the scope of the center's operations. The Governance Board will review OCTIC Privacy Policy and any subsequent changes.

OCTIC also utilizes a Privacy Officer who is selected by the General Counsel of the Oklahoma Department of Public Safety. The Privacy Officer receives reports regarding alleged errors and violations of the provisions of this policy and monitors the center's interaction with the Information Sharing Environment, ensuring privacy, civil rights, and civil liberties protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy-enhancing technologies. The Privacy Officer can be contacted at Privacy.Officer@dps.ok.gov.

## IV. Information

### A. Seeking or Retaining Information

OCTIC will seek or retain information, subject to conditions articulated in Subsection IV(B), that:

- Is based on a possible threat to public safety or the enforcement of criminal law, or
- Is based on reasonable suspicion that an identifiable individual or organization is involved in a definable criminal activity or enterprise 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

- Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime, or
- Is useful in crime analysis or in the administration of criminal justice and public safety (including topical searches), and
- The source of the information is reliable and verifiable or limitations on the quality of the information are identified, and
- To OCTIC's best information and belief was obtained lawfully.

The center may retain protected information based on a level of suspicion that is less than "reasonable suspicion," such as tips, leads and suspicious activity report [SAR] information subject to the procedures specified in this policy.

### B. Limitation on Seeking or Retaining Information

In accordance with applicable laws, guidance, and regulations, OCTIC will not seek or retain and will inform participating agencies not to submit information about individuals or organizations solely based on their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, national origin, ages, disabilities, genders, gender identities, or sexual orientations.

When participating on a federal law enforcement task force or when documenting a SAR or an ISE-SAR in the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI), race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity must not be considered as factors creating suspicion. However, those attributes may be documented in specific suspect descriptions for identification purposes.

### C. Handling Notices and Labels

OCTIC will attach (or ensure the originating agency has attached) specific handling notices, labels, or descriptive metadata to information used, accessed, or disseminated to clearly indicate any restrictions on information sharing based on information sensitivity or classification.

Additionally, where appropriate, OCTIC applies labels to center-originated information (or ensures that the originating agency has applied labels) to indicate to the accessing authorized user that information is subject to federal or state laws restricting access, use, or disclosure.

### D. Categorization of Information

OCTIC personnel will, when appropriate, assess information upon receipt to determine or review its nature, usability, and quality. Personnel will assign categories to the information (or

ensure the originating agency has assigned categories to the information) to reflect the assessment, such as:

- Whether the information consists of tips and leads (including SAR data), criminal history, intelligence information, case records, conditions of supervision, case progress, or other information category.
- The nature of the source as it affects veracity (for example, anonymous tip, trained interviewer or investigator, public record, private sector).
- The reliability of the source (for example, reliable, usually reliable, unreliable, unknown).
- The validity of the content (for example, confirmed, probable, doubtful, cannot be judged).

### E. Labeling of Protected Information

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

- Protect confidential sources and police undercover techniques and methods.
- Not interfere with or compromise pending criminal investigations.
- Provide legally required protections based on the individual's status.

Labels assigned to existing information will be reevaluated whenever:

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

### F. Processing Tips, Leads, and SARs

OCTIC 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 (including SAR information). Center personnel will:

- Prior to allowing access to or dissemination of the information, attempt, where appropriate, to validate or refute the information and assess the information for sensitivity and confidence by subjecting it to an evaluation or screening process to determine its credibility and value and categorize the information as unsubstantiated or uncorroborated if attempts

to validate or determine the reliability of the information have been unsuccessful. The center will use a standard reporting format for SAR information.

- Store the information using the same storage method used for data that rises to the level of reasonable suspicion and includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information.
- Allow access to or disseminate the information using the same (or a more restrictive) access or dissemination standard used for data that rises to the level of reasonable suspicion (for example, "need-to-know" and "right-to-know" access or dissemination of PII).
- 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, provided all such disseminations to non-law enforcement persons or entities shall first be approved by the OCTIC Director.
- Retain information for no more than twelve months in order to work an unvalidated tip or lead to determine its credibility and value or assign a "disposition" label (for example, undetermined or unresolved, cleared or unfounded, verified, or under active investigation) so a subsequently authorized user knows the status and purpose for the retention and will retain the information based on the retention period associated with the disposition label.
- Adhere to and follow the center's physical, administrative, and technical security measures to ensure the protection and security of tips, leads, and SAR information. Tips, leads, and SAR information will be secured in a system that is the same as or similar to the system that secures data that rises to the level of reasonable suspicion.

OCTIC 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.

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

### G. Record of Sources

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

## V. Acquiring and Receiving Information

### A. Information Gathering

Information-gathering and investigative techniques used by OCTIC will adhere to applicable laws and guidance, including 28 C.F.R. Part 23 regarding "criminal intelligence information," as applicable, and applicable federal and state constitutional and statutory provisions.

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

- An individual who, or nongovernmental entity that, OCTIC knows may receive a fee or benefit for providing the information, except as expressly authorized by law or center policy.
- An individual who, or information provider that, OCTIC knows is legally prohibited from obtaining or disclosing the information.

### B. Evaluation of ISE-SAR Information Submitted to OCTIC

Law enforcement officers and appropriate center and participating agency staff members will be trained to recognize those behaviors and incidents that are indicative of criminal activity associated with terrorism. OCTIC's SAR process includes safeguards to ensure, to the greatest degree possible, only information regarding individuals involved in activities that have been determined to be consistent with criminal activities associated with terrorism will be documented and shared through the ISE. These safeguards are intended to ensure information that could violate civil rights (race, ethnicity, national origin, religion, etc.) and civil liberties (speech, assembly, association, religious exercise, etc.) will not be intentionally or inadvertently gathered, documented, processed, and shared.

## VI. Information Quality Assurance

### A. Information Evaluation

OCTIC will make every reasonable effort to ensure information gathered, developed, and retained by OCTIC is derived from dependable and trustworthy sources; accurate; current; complete, including the relevant context in which it was sought or received and other related

information; and merged with other information about the same individual or organization only when the applicable standard (see Section VIII. Merging and Combining Records) has been met.

### B. Information Labeling

At the time of retention in the system, the information will be labeled regarding its level of quality (accuracy, completeness, currency, and confidence [verifiability and reliability]).

The labeling of retained information will be reevaluated by OCTIC or the originating agency when new information is gathered that has an impact on confidence (source reliability and content validity) in previously retained information.

### C. Information Originating from External Agencies

Originating agencies external to OCTIC are responsible for reviewing the quality and accuracy of the data provided to the center. OCTIC will review the quality of information it has received from an originating agency and advise the appropriate contact person in the originating agency, in writing or electronically, if its data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable.

### D. Information Found to be Inaccurate

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

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

### E. Quality Assurance for SARs

OCTIC will put in place a process for additional fact development during the vetting process where a SAR includes PII and is based on behaviors that are not inherently criminal. OCTIC will articulate additional facts or circumstances to support the determination that the behavior observed is not innocent but rather reasonably indicative of preoperational planning associated with terrorism.

## VII. Analysis

Information acquired or received by OCTIC or accessed from other sources will be analyzed only by qualified and properly trained individuals who have successfully completed OCTIC's criminal history and background screening. Information subject to collation and analysis is information as defined and identified in Section IV. Information.

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

- Further crime prevention (including terrorism), law enforcement, public safety, force deployment, or prosecution objectives and priorities established by the center.
- 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.

## VIII. Merging and Combining Records

Records about an individual or an organization from two or more sources will not be merged by OCTIC unless there is sufficient identifying information to clearly establish 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 a higher accuracy of match. Records may be merged only by, or with the approval of, the Analyst Supervisor.

## IX. Access, Sharing, and Disclosure

### A. ISE-SARs

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

### B. Access to Records

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

## C. Dissemination of Records or Information

### *1. Criminal Intelligence Information*

OCTIC shall disseminate criminal intelligence information only where there is a need to know and a right to know the information in the performance of a law enforcement activity.

- Except as noted in the following paragraph, OCTIC shall disseminate criminal intelligence information only to law enforcement authorities who shall agree to follow procedures regarding information receipt, maintenance, security, and dissemination which are consistent with these principles.
- This section shall not limit the dissemination of an assessment of criminal intelligence information to a government official or to any other individual, when necessary, to avoid imminent danger to life or property.

An audit trail sufficient to allow the identification of each individual who accessed or received information retained by the center and the nature of the information accessed will be kept by the center.

### *2. Other OCTIC Records*

Records retained by OCTIC that do not qualify as criminal intelligence information may be accessed by or *disseminated to those responsible for public protection, public safety, or public health* only for public protection, public safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures. An audit trail sufficient to allow the identification of each individual who accessed or received information retained by the center and the nature of the information accessed will be kept by the center.

### *3. Requests for Information*

Information gathered or collected and records retained by OCTIC may be accessed or disseminated for specific purposes upon request by persons authorized by law to have such access and only for those uses and purposes specified in the law. An audit trail sufficient to allow the identification of each individual who requested, accessed, or received information retained by the center; the nature of the information requested, accessed, or received; and the specific purpose will be kept with the record/information disseminated for the remainder of the lifecycle of that record.

Agencies and individual recipients may not disseminate information accessed or disseminated from the center without approval from the center or other originator of the information.

### D. Public Disclosures

Information gathered or collected and records retained by OCTIC may be accessed or disclosed to a member of the public only if the information is subject to disclosure under the Oklahoma Open Records Act (51 O.S. § 24A.1, *et seq*.) or otherwise appropriate for release to further the center's mission and is not exempt from disclosure by law. An audit trail sufficient to allow the identification of the nature of the information received and each member of the public who received the information will be kept by the center.

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

- Records required to be kept confidential by law are exempted from disclosure requirements of the Oklahoma Open Records Act. *See* 51 O.S. § 24A.5(1) (recognizing the Open Records Act "does not apply to records specifically required by law to be kept confidential . . . ."). For example, 28 C.F.R. Part 23 limits disclosure of criminal intelligence information.
- Information determined by the federal government to meet the definition of "classified information" as defined in the National Security Act, Public Law 235, Section 606, and in accordance with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010.
- Law enforcement records that are exempted from mandatory disclosure requirements. *See* 51 O.S. § 24A.8.
- Certain records pertaining to terrorism are exempt from mandatory disclosure. *See* 51 O.S. § 24A.28.

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

Information gathered or collected and records retained by OCTIC will not be sold, published, exchanged, or disclosed for commercial purposes.

### E. Pre-Dissemination/Disclosure Review

To promote appropriate privacy, civil rights, and civil liberties protections, OCTIC requires review and approval by the Privacy Officer and the OCTIC Director (or Director's designee) prior to dissemination or disclosure of all OCTIC analytical products and all disseminations and re-disseminations containing personally identifiable information. Provided, an analyst may, without pre-approval, forward an unedited tip, lead, or SAR directly to the affected law enforcement agency, public safety agency, or school if the analyst does not include additional analysis, or may

disseminate Oklahoma Department of Public Safety Emergency Alerts (such as AMBER alerts or endangered missing person alerts).

## X. Disclosure to Individuals and Corrections

Persons or entities may submit requests to Privacy.Officer@dps.ok.gov to inquire of the existence, and request opportunity to review, the information about him or her that has been gathered and retained by OCTIC. OCTIC will not reveal the existence, content, and source of information to an individual when the information is not subject to mandatory disclosure pursuant to the Oklahoma Open Records Act (51 O.S. § 24A.1 *et seq.*) or the information is otherwise required by law to be kept confidential. Examples may include:

- Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution. *See* 51 O.S. § 24A.8.
- Disclosure would endanger the health or safety of an individual, organization, or community. *See* 51 O.S. § 24A.28.
- The information is in a criminal intelligence information system subject to 28 C.F.R. Part 23. *See* 28 C.F.R. § 23.20(e).
- The information relates to terrorism. *See* 51 O.S. § 24A.28.
- The information is required by state or federal law to be kept confidential.

For information otherwise subject to disclosure pursuant to the Oklahoma Open Records Act and other applicable laws, OCTIC will adhere to the Open Records Act inspection and copying procedures of the Oklahoma Department of Public Safety.

If a person or entity disputes the accuracy of any information disclosed by OCTIC about that person or entity, they may submit to Privacy.Officer@dps.ok.gov a record describing the inaccuracy, and OCTIC will add that record to its file.

## XI. Security Safeguards

The OCTIC Director will appoint a security officer who will guide OCTIC in maintenance of physical security, systems security, and operational security.

OCTIC will operate in a secure facility protected from external intrusion. The center will utilize secure internal and external safeguards against network intrusions. Access to the center's databases from outside the facility will be allowed only over secure networks.

### A. OCTIC Criminal Intelligence System(s)

OCTIC will secure tips, leads, and SAR information 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 C.F.R. Part 23.

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

Access to OCTIC criminal intelligence system(s) will be granted only to personnel employed by, or detailed to OCTIC, whose positions and job duties require such access; who have completed OCTIC's criminal history and background screening process; who possess an appropriate security clearance, if applicable; and who have been selected, approved, and trained accordingly. Credentialed, role-based access controls will be used by OCTIC to control the information to which a particular group or class of users can have access based on the group or class.

Queries made to OCTIC's criminal intelligence system(s) will be logged into the data system identifying the user initiating the query.

### B. Security Breaches

All personnel employed by, or detailed to, OCTIC shall report a suspected or confirmed breach to the Privacy Officer as soon as possible and without unreasonable delay, consistent with applicable laws, regulations, policies, and procedures. This includes a breach in any medium or form, including paper, oral, and electronic.

To the extent allowed by existing data breach notification law, following assessment of the suspected or confirmed breach and as soon as practicable, OCTIC will notify the originating agency from which the center received PII of the nature and scope of a suspected or confirmed breach of such information.

OCTIC's response to data breaches will be guided by the Security Breach Notification Act, 24 O.S. §§ 161-166. OCTIC will determine whether a data breach requires notification to an affected individual, in accordance with applicable laws, regulations, policies, and procedures.

## XII. Information Retention and Destruction

All tips, tasks, leads, and SARs addressing allegations of criminal activity by an individual or entity, which are based on a level of suspicion that is less than "reasonable suspicion," will be reviewed for record retention (validation or purge) by OCTIC at least every twelve months.

All criminal intelligence information, as that term is defined in 28 C.F.R. § 23.3, will be reviewed for record retention (validation or purge) by OCTIC at least every five years, in accordance with 28 C.F.R. § 23.20.

For other information or intelligence, the record retention will be established by state law or local ordinance, or in accordance with 595 O.A.C. § 1-9-10.

OCTIC will delete information once its retention period has expired as provided by this policy.

## XIII. Accountability and Enforcement

### A. Information System Transparency

OCTIC's P/CRCL policy will be posted at https://oklahoma.gov/dps/octic.html.

OCTIC's Privacy Officer will be responsible for receiving and processing inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s) maintained or accessed by the center. The Privacy Officer can be contacted at Privacy.Officer@dps.ok.gov.

### B. Accountability

OCTIC will maintain an audit trail of accessed, requested, or disseminated information.

OCTIC personnel or other authorized users shall report errors and suspected or confirmed violations of center policies relating to protected information to the center's Privacy Officer.

OCTIC may, with or without notice, conduct an audit and inspection of the information and intelligence contained in its information system(s) and may include any type of medium (printed and electronic) or technology (e.g., physical servers, virtual machines, and mobile devices) used in a work-related OCTIC activity.

The audit(s) may be conducted by OCTIC's Privacy Officer, Director, or Assistant Director. The auditor may conduct a random audit, without announcement, at any time and without prior notice to staff of the center. The audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the center's information and intelligence system(s).

OCTIC, guided by the appointed and trained Privacy Officer, will review and update the provisions protecting privacy, civil rights, and civil liberties contained in this policy annually and will make appropriate changes in response to changes in applicable law, technology, and the purpose and use of the information systems.

### C. Enforcement

If an authorized user or participating agency 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 OCTIC Director will:

- Suspend or discontinue access to information by the authorized user or the participating agency.
- For OCTIC personnel, adhere to DPS Administrative Investigations and Progressive Discipline polices.
- For authorized users detailed to OCTIC from another agency, address the matter with the authorized user's chain of command and, if appropriate, suspend or terminate the user's participation in OCTIC.
- Refer the matter to appropriate authorities for criminal investigation, as necessary, to effectuate the purposes of the policy.

OCTIC, subject to its sole discretion and without notice, reserves the right to restrict the qualifications and number of personnel having access to center information and to suspend or withhold service and deny access to OCTIC criminal intelligence systems and other information systems to OCTIC personnel, any participating agency, or participating agency personnel.

## XIV. Training

OCTIC will require the following individuals to participate in training programs regarding implementation of and adherence to this P/CRCL policy:

- All center personnel.
- Participating agency personnel.
- Staff members in other public agencies or private contractors providing services to the center.
- Authorized users who are not employed by the center or a contractor.

OCTIC's P/CRCL policy training program will cover:

- Purposes of the P/CRCL protection policy.
- Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the center.

- How to implement the policy in the day-to-day work of the user.
- The potential impact of violations of the agency's P/CRCL policy.
- Mechanisms for reporting violations of center P/CRCL protection policies and procedures.
- How to identify, report, and respond to a suspected or confirmed breach of PII.
- The nature and possible penalties for policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.
- Updates to the P/CRCL policy, if any, in response to changes in law and implementation experience.
- ISE Core Awareness Training.

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

## Appendix A

OKLAHOMA COUNTER TERRORISM INTELLIGENCE CENTER
Oklahoma's Fusion Center

### OCTIC PRIVACY POLICY ACKNOWLEDGEMENT

I certify I have been provided with the Oklahoma Counter Terrorism Intelligence Center's Privacy Policy, I have reviewed the Privacy Policy, and I agree to comply with the Privacy Policy at all times while performing functions in and/or for the fusion center.

Signature: _____

Name: _____

Title: _____

Employing Agency: _____

Date: _____

# Appendix B

## DEFINITIONS

The following is a list of definitions for terms used within this policy and within the Information Sharing Environment context.

**Access—**Information access is being able to get to (usually having permission to use) particular information on a computer. Web access means having a connection to the Internet through an access provider or an online service provider.

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.

**Analysis (law enforcement)—**The review of information and its comparison to other information to determine the meaning of the data in reference to a criminal investigation or assessment.

**Audit Trail—**A generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail—what commands were issued to the system, what records and files were accessed or modified, etc.

Audit trails are a fundamental part of computer security used to trace (albeit usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

**Center—**Refers to the Oklahoma Counter Terrorism Intelligence Center ("OCTIC").

**Civil Liberties—**According to the U.S. Department of Justice's Global Justice Information Sharing Initiative, 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.[1] 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.

**Civil Rights—**The term "civil rights" refers to those rights and privileges of equal protection that government entities must afford to all individuals in the United States regardless of race, ethnicity, gender, national origin, religion, sexual orientation, gender identity, or other characteristics unrelated to the worth of the individual. Protection of civil rights means that government entities will take action to ensure that individuals are not discriminated against on the basis of any federally or state protected characteristic. For example, a state may have constitutional or statutory language

[1] Civil Rights and Civil Liberties Protections Guidance, at 4 (August 2008).

regarding parental status. Generally, the term "civil rights" involves positive (or affirmative) government action to protect against infringement, while the term "civil liberties" involves restrictions on government.[2]

**Collect—**For purposes of this document, "gather" and "collect" mean the same thing.

**Confidentiality—**Refers to the obligations of individuals and institutions to appropriately use information and data under their control once they have been disclosed to them and in accordance with applicable data security laws and policies.

**Criminal Activity—**A behavior, an action, or an omission that is punishable by criminal law.

**Criminal Intelligence Information—**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 activity. Criminal intelligence records are maintained in a criminal intelligence system per 28 C.F.R. Part 23.

**Data—**Inert symbols, signs, descriptions, or measures; elements of information.

**Data Breach—**The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for a purpose other than the authorized purpose.

The center's response to a data breach may be addressed in state law or agency policy. This may include incidents such as:

- Theft or loss of digital media—including computer tapes, hard drives, or laptop computers containing such media—upon which such information is stored unencrypted; posting such information on the Internet.
- Unauthorized employee access to certain information.
- Moving such information to a computer otherwise accessible from the Internet without proper information security precautions.
- Intentional or unintentional transfer of such information to a system that is not completely open but is not appropriately or formally accredited for security at the approved level.
- Transfer of such information to the information systems of a possibly hostile agency or an environment where it may be exposed to more intensive decryption techniques.

**Disclosure—**The release, transfer, provision of access to, sharing, publication, or divulging of PII in any manner—electronic, verbal, or in writing—to an individual, agency, or an 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.

**Evaluation**—An assessment of the reliability of the source and accuracy of the raw data.

**Fair Information Practice Principles (FIPPs)—**FIPPs are a set of internationally recognized principles that inform information privacy policies both within government and the private sector. Although specific articulations of the FIPPs vary and have evolved since their genesis in the 1970s, core elements are consistent among nations, states, and economic sectors. These core elements are incorporated into information privacy laws, policies, and governance documents around the world. They provide a description of underlying privacy and information exchange principles and a simple framework for proper use that needs to be done with regard to privacy in integrated justice systems. Because of operational necessity, it may not always be possible to apply all of the principles equally. For example, the Individual Participation Principle (#8) may be of limited applicability in intelligence operations, as fusion centers

[2] The definition of "civil rights" is a modified version of the definition contained in the *National Criminal Intelligence Sharing Plan* (NCISP), at pp. 5–6, and Civil Rights and Civil Liberties Protections Guidance, at 5.

do not generally engage with individuals. While the FIPPs do not apply to OCTIC in all respects and do not represent a governing document for OCTIC, OCTIC's P/CRCL policy is informed by the FIPPs.

**Fusion Center**—Defined in the ISE-SAR Functional Standard, Version 1.5.5 as "[a] collaborative effort of two or more Federal, State, local, tribal, or territorial (SLTT) government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity." (Source: Section 511 of the 9/11 Commission Act). State and major urban area fusion centers serve as focal points within the State and local environment for the receipt, analysis, gathering, and sharing of threat-related information between the federal government and SLTT and private sector partners.

**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.

**Information Sharing Environment (ISE**)—In accordance with Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended, the ISE is a conceptual framework composed of the policies, procedures, and technologies linking the resources (people, systems, databases, and information) of SLTT agencies; federal agencies; and the private sector to facilitate terrorism-related information sharing, access, and collaboration.

**Information Sharing Environment (ISE) Suspicious Activity Report (SAR) (ISE-SAR)—**An ISE-SAR is a SAR that has been determined, pursuant to a two-step process established in the ISE-SAR Functional Standard, to have a potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism).

**Law Enforcement Information—**For purposes of the ISE, law enforcement information means any information obtained by or of interest to a law enforcement agency or official that is both (a) related to terrorism or the security of our homeland and (b) relevant to a law enforcement mission, including but not limited to information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of or response to criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of or response to criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance.

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

**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.

**Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)—**The NSI establishes standardized processes and policies that provide the capability for federal, SLTT, campus, and railroad law enforcement and homeland security agencies to share timely, relevant ISE-SARs through a distributed information sharing system that protects privacy, civil rights, and civil liberties.

**Nationwide SAR Initiative (NSI) SAR Data Repository (SDR)—**The NSI SDR consists of a single data repository, built to respect and support originator control and local stewardship of data, which incorporates federal, state, and local retention policies. Within the SDR, hosted data enclaves extend this approach to information management and safeguarding practices by ensuring a separation of data across participating agencies.

**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 to perform or assist in a law enforcement, homeland security, or counterterrorism activity or other lawful and authorized government activity, such as to further an investigation or meet another law enforcement requirement.

**Originating Agency—**The agency or organizational entity that documents information or data, including source agencies that document SAR (and, when authorized, ISE-SAR) information that is collected by a fusion center.

**Participating Agency—**An organizational entity that is authorized to access or receive and use center information and/or intelligence databases and resources for lawful purposes through its authorized individual users.

**Personally Identifiable Information (PII)—**Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."

**Preoperational Planning—**As defined in ISE-SAR Functional Standard, Version 1.5.5, "preoperational planning describes activities associated with a known or particular planned criminal operation or with terrorist operations generally."

**Privacy—**Refers to avoidance of the inappropriate collection, use, and release of PII.

**Purge—**A term that is commonly used to describe methods that render data unrecoverable in a storage space or to destroy data in a manner that it cannot be reconstituted.

**Reasonably Indicative—**This operational concept for documenting and sharing suspicious activity takes into account the circumstances in which that observation is made which creates in the mind of the reasonable observer, including a law enforcement officer, an articulable concern that the behavior may indicate preoperational planning associated with terrorism or other criminal activity. It also takes into account the training and experience of a reasonable law enforcement officer, in cases in which an officer is the observer or documenter of the observed behavior reported to a law enforcement agency.

**Record—**Any item, collection, or grouping of information that includes PII and is collected, received, accessed, used, disseminated, retained, and purged by or for the collecting agency or organization.

**Right to Know—**A requirement for access to specific information to perform or assist in a lawful and authorized governmental function. Right to know is determined by the mission and functions of a law enforcement, homeland security, counterterrorism, or other lawful and authorized government activity or the roles and responsibilities of particular personnel in the course of their official duties.

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

**Source Agency/Organization—**Defined in the ISE-SAR Functional Standard, Version 1.5.5, source agency refers to the agency or entity that originates the SAR (examples include a local police department, a private security firm handling security for a power plant, and a security force at a military installation). The source organization will not change throughout the life of the SAR.

**Submitting Agency/Organization—**The organization that actuates the push of the ISE-SAR to the NSI community. The submitting organization and the source organization may be the same.

**Suspicious Activity—**Defined in the ISE-SAR Functional Standard, Version 1.5.5 as "[o]bserved behavior reasonably indicative of preoperational planning associated with terrorism or other criminal activity." Examples of suspicious activity include surveillance, photography of sensitive infrastructure facilities, site breach or physical intrusion, cyberattacks, testing of security, etc.

**Suspicious Activity Report (SAR)—**Defined in the ISE-SAR Functional Standard, Version 1.5.5 as "[o]fficial documentation of observed behavior reasonably indicative of preoperational planning associated with terrorism or other criminal activity." Suspicious activity report (SAR) information offers a standardized means for feeding information repositories or data analysis tools. Patterns identified during SAR information analysis may be investigated in coordination with the reporting agency and, if applicable, a state or regional fusion center. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor is it designed to support interagency calls for service.

**Terrorism Information—**Consistent with Section 1016(a)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), all information relating to (a) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or materials support, or activities of foreign **or** international terrorist groups or individuals **or** of domestic groups **or** individuals involved in transnational terrorism; (b) threats posed by such groups or individuals to the United States, United States persons, or United States interests or to those interests of other nations; (c) communications of or by such groups or individuals; or (d) other groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

Weapons of Mass Destruction (WMD) information was defined and included in the definition of "terrorism information" by P.L. 110-53.

**Terrorism-Related Information—**In accordance with the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended by the 9/11 Commission Act (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 the 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 may include intelligence information.

**Tips and Leads Information or Data—**Generally uncorroborated reports or information generated from inside or outside a law enforcement agency that allege or indicate some form of possible criminal activity. Tips and leads are sometimes referred to as suspicious incident report (SIR), suspicious activity report (SAR), and/or field interview report (FIR) information. However, SAR information should be viewed, at most, as a subcategory of tip or lead data. Tips and leads information does not include incidents that do not have a criminal offense attached or indicated, criminal history records, or CAD data.

A tip or lead can come from a variety of sources, including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information may be based on mere suspicion or on a level of suspicion that is less than "reasonable suspicion" and, without further information or analysis, it is unknown whether the information is accurate or useful. Tips and leads information falls between being of little or no use to law enforcement and being extremely valuable depending on the availability of time and resources to determine its meaning.

**U.S. Person—**Executive Order 12333 states that a "United States person" means a United States citizen, an alien known by the intelligence element 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.

**User—**An individual representing a participating agency who is authorized to access OCTIC's information and intelligence databases and resources for lawful purposes.