# *Oregon TITAN Fusion Center*

# PRIVACY POLICY

## 1.0 Purpose

The Oregon TITAN Fusion Center (the Center) was initiated in response to the increased need for timely information sharing and exchange of terrorism and crime-related information among members of the Oregon law enforcement community. The purpose of the Center is to protect the citizens of the State of Oregon from terrorism activity by providing an all-crimes information clearinghouse for federal, state, local and tribal law enforcement agencies.

The Center is a collaborative effort of state and federal law enforcement agencies to provide resources, expertise, and information to the law enforcement community with the goal of maximizing the ability to detect, disrupt, prevent, and respond to terrorism, organized crime, and gang-related criminal activity.

One component of the Oregon TITAN Fusion Center focuses on the development and exchange of information, including criminal intelligence. This component focuses on the process whereby information is collected, integrated, evaluated, analyzed and disseminated. The Oregon law enforcement community recognizes that combining intelligence resources will allow greater dissemination of intelligence products and will greatly enhance the ability to predict, prevent, and respond to terrorist threats and related criminal activity within the state. Law enforcement agencies also recognize the role of intelligence sharing in avoiding conflicting operational activities that may endanger officers and civilians.

The information received and maintained by the Oregon TITAN Fusion Center is provided on a voluntary basis by "participating agencies," or is information obtained by the Center from other sources such as other law enforcement agencies, "open" media sources, commercial databases, public records and unclassified government material. The Oregon TITAN Fusion Center will keep a record of the source of all information sought and collected by the Center. "Participating agencies" are those which have assigned personnel to work at the Center and have entered into a Memorandum of Understanding. The Oregon TITAN Fusion Center's products and services will be made available to local, state, and federal law enforcement agencies operating in Oregon and to other entities as permitted by this Privacy Policy (Policy).

The purpose of this privacy, civil rights, and civil liberties protection policy is to promote Oregon TITAN and user conduct that complies with applicable federal, state, local, and tribal law (see Appendix A, Terms and Definitions, of this policy)] and assists the Center and its 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 physical or financial 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 the criminal investigatory, criminal intelligence, and justice system processes and information.

7. Minimizing reluctance of individuals or groups to use or cooperate with the justice system.

## 2.0 Compliance with Laws Regarding Privacy, Civil Rights, and Civil Liberties

All participating agency personnel, personnel providing information technology services to the Oregon TITAN Fusion Center, private contractors, and users (including Information Sharing Environment [ISE] participating centers and agencies) will comply with the provisions contained in this Policy and with all applicable laws protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing, and disclosure of information as stated below and herein.

The internal operating policies governing the operation of the Oregon TITAN Fusion Center comply with 28 CFR Part 23, ORS 181.575, the Oregon Department of Justice Administrative Rules 137-090- 0000-0225, ORS Chapter 192 relating to public records, the U.S. and Oregon constitutions, and state and federal law pertaining to confidential records and records containing personally identifiable information.

The Center's Executive Advisory Committee has approved this Policy and oversees its implementation in various ways including: liaising with the community to ensure that privacy and civil rights are protected as provided in this policy and by the Center's information-gathering and collection, retention, and dissemination processes and procedures; and conducting an annual review and recommendation for updates to the policy, with the assistance of the Privacy Officer, in response to changes in law and implementation experience, including the results of audits and inspections. The Director for the Center is responsible for insuring that all participating agency personnel, personnel providing information technology services to the Oregon TITAN Fusion Center, private contractors, and users will comply with the terms of this Policy. Section 9 of this Policy contains specific provisions relating to the review, implementation and enforcement of this Policy.

The Privacy Officer, who is the attorney for the Center and who is appointed by the Chief Counsel of the Oregon Department of Justice Criminal Division, receives reports regarding alleged errors and violations of the provisions of this policy, receives and coordinates complaint resolution under the Center's redress policy, and serves as the liaison for the Information Sharing Environment, ensuring that privacy 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 the following address: 610 Hawthorne Ave, SE, Suite 210, Salem, Oregon, 97301, oregonfusioncenter@doj.state.or.us.

The Director of the Oregon TITAN Fusion Center ensures that enforcement procedures and sanctions outlined in Section 9.3 are adequate and enforced.

## 3.0 Definitions

Appendix A provides definitions for words or phrases regularly used in this Policy to explain their meaning in the context of this Policy.

## 4.0 Seeking, Collecting, and Retaining Information and Criminal Intelligence

Each participating agency will determine which database(s) it will provide, and access to such database(s) will be governed by the laws that govern the particular agency respecting such data, as well as by applicable federal laws.

Because the laws governing information that can be sought, collected or released on private individuals will vary from agency to agency, limitations on the collection of data concerning individuals is the responsibility of the collector of the original source data. Each contributor of information will abide by the collection limitations applicable to it by reason of law. Information contributed to the Oregon TITAN Fusion Center should be that which has been collected in conformance with those limitations.

The following provisions set out the policies that will guide the operation of the Oregon TITAN Fusion Center in four areas: 1) the types of information that may be sought and the types of information that may be collected or retained; 2) information that may not be sought, collected, or retained; 3) permissible methods of seeking information, including the receipt of information from third parties in the form of unsolicited tips; and 4) assessing information with respect to its validity, reliability, and access or disclosure.

### 4.1 Information That May Be Sought or Retained

1. The Oregon TITAN Fusion Center will seek or retain information only under the following circumstances:
    a. The source of the information is reliable and verifiable or limitations on the quality of the information are identified; and
    b. The information was collected in a fair and lawful manner, with the knowledge and consent of the individual, if appropriate, and
    c. The information is based on a possible threat to public safety or the enforcement of the criminal law; or
    d. Where there is reasonable suspicion that a specific individual or organization has committed a criminal offense or is involved in or is planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation, and the information is relevant to the criminal (including terrorist) conduct or activity; or
    e. The information 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
    f. The information is useful in crime analysis or in the administration of criminal justice and public safety (including topical searches).

2. Collection, retention and storage of criminal intelligence will comply with applicable state and federal law. The Center may retain protected information that is based on a level of suspicion that is less than "reasonable suspicion," such as tips and leads or suspicious activity report (SAR) information, subject to the policies and procedures specified in this policy.

3. The Oregon TITAN Fusion Center will not seek or retain information about an individual or organization solely on the basis of their religious, political, racial, or social views or activities; their participation in a particular non-criminal organization or lawful event; or their race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation.

4. The Oregon TITAN Fusion Center shall apply labels to center-originated information (or ensures that the originating agency has applied labels) to indicate to the accessing authorized user that:
    a. The information is "protected information" to include "personal data" on any individual (see Definitions), and, to the extent expressly provided in this policy, includes organizational entities.

5. The information is subject to ORS 181.575, ORS 192.410-192.505, OAR 137-090-0000, et seq., 28 CFR Part 23, the United States Constitution and the Oregon Constitution restricting access, use or disclosure.

6. The Oregon TITAN Fusion Center personnel will, upon receipt of information, assess the information to determine or review its nature, usability, and quality. Personnel will assign categories to the information (or ensure that the originating agency has assigned categories to the information) to reflect the assessment, such as:
    a. Whether the information consists of tips and leads data, suspicious activity reports, criminal history, intelligence information, case records, conditions of supervision, case progress, or other information category.
    b. The nature of the source as it affects veracity (for example, anonymous tip, trained interviewer or investigator, public record, private sector).
    c. The reliability of the source (for example, reliable, usually reliable, unreliable, unknown).
    d. The validity of the content (for example, confirmed, probable, doubtful, cannot be judged).

7. The Oregon TITAN Fusion Center will keep a record of the source of all retained information.

8. Tips and Leads Information or Data: The Oregon TITAN Fusion Center may seek or retain information of uncorroborated information or reports generated from inside or outside the agency that alleges or indicates some form of possible criminal activity. Tips and leads may include suspicious incidents reports (SIR) information, suspicious activity report (SAR) information, 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 should be maintained in a secure system, similar to data that rises to the level of reasonable suspicion.

9. 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 raises some suspicion but may be based on a level of suspicion that is less than "reasonable suspicion" and, 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. Center 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. Center personnel will:
    a. Prior to allowing access to or dissemination of the information, ensure that attempts to validate or refute the information have taken place and that the information has been assessed for sensitivity and confidence by subjecting it to an evaluation or screening process to determine its credibility and value and categorize the information as unsubstantiated or uncorroborated if attempts to validate or determine the eligibility of the information have been unsuccessful. The Center will use a standard reporting format and standard collection codes for SAR information.
    b. Store the information using the same storage method used for data which rises to the level of reasonable suspicion and which 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 for personally identifiable information).
    d. Regularly provide access to or disseminate the information in response to an interagency inquiry for law enforcement, homeland security, or public safety and analytical purposes or provide an assessment of the information to any agency, entity, individual, or the public when credible information indicates potential imminent danger to life or property.
    e. Retain information for one hundred and eighty (180) days in order to work an unvalidated tip, lead, or SAR information to determine its credibility and value or assign a "disposition" label (for example, undetermined or unresolved, cleared unfounded, verified, or under active investigation) so that 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. An additional one hundred and eighty (180) day retention may be authorized by the Director of the Center, after consultation with Privacy Officer, if after the first one hundred and eighty (180) days, it appears likely that based upon investigation during the first one hundred and eighty (180) days the unvalidated tip, lead, or SAR information may be credible.
    f. 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.

10. The Oregon TITAN Fusion Center 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.

11. The Oregon TITAN Fusion Center 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. Further, the Center will provide notice mechanisms, including but not limited to metadata or data field labels that will enable ISE authorized users to determine the nature of the protected information and how to handle the information in accordance with applicable legal requirements.

12. The Oregon TITAN Fusion Center requires certain basic descriptive information (metadata tags or labels) to be entered and electronically associated with data (or content) for which there are special laws, rules, or policies regarding access, use, and disclosure, including terrorism-related information shared through the ISE. The types of information include:
    a. The name of the originating Center, department or agency, component, and subcomponent.
    b. The name of the Center's justice information system from which the information is disseminated.
    c. The date the information was collected and, where feasible, the date its accuracy was last verified.
    d. The title and contact information for the person to whom questions regarding the information should be directed.

13. The Oregon TITAN Fusion Center will attach (or ensure that the originating agency has attached) specific labels and descriptive metadata to information that will be used, accessed, or disseminated to clearly indicate any legal restrictions on information sharing based on information sensitivity or classification.

## 4.2 Methods of Seeking or Receiving Information

1. Information gathering and investigative techniques used by the Oregon TITAN Fusion Center will comply with all applicable laws, including but not limited to ORS 181.575, OAR 137-090-0000, et seq., 28 CFR Part 23, the United States Constitution and the Oregon Constitution.

2. The Oregon TITAN Fusion Center's SAR process provides for human review and vetting to ensure that information is both legally gathered and, where applicable, determined to have a potential terrorism nexus. Law enforcement officers and

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

3. The Oregon TITAN Fusion Center's SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved in activities that have been determined to be consistent with criminal activities or associated with terrorism will be documented and shared through the ISE. These safeguards are intended to ensure that information that could violate civil rights (race, religion, national origin, ethnicity, etc.) and civil liberties (speech, assembly, religious exercise, etc.) will not be intentionally or inadvertently gathered, documented, processed, and shared.

4. The Oregon TITAN Fusion Center will not directly or indirectly seek, receive or retain information from:
    a. An individual or nongovernmental information provider, who may or may not receive a fee or benefit for providing the information, except as expressly authorized by law or Oregon TITAN Fusion Center policy.
    b. An individual or information provider who is legally prohibited from obtaining the specific information sought or disclosing it to the Center.
    c. An individual or information provider who used methods for collecting the information that the Center itself could not legally use, except where:
        i. The information was provided through an anonymous tip, in which case the Center may use the information as a basis to investigate further, but shall not retain the information unless it meets the requirements set out in Section 4.1; or
        ii. The information was provided by a cooperating defendant or criminal informant and the person was not acting at the direction or under the control of the Center; and
        iii. The commercial database entities provide a written assurance that their methods for gathering personally identifiable information comply with applicable local, state, tribal, territorial, and federal laws, statutes, and regulations and that these methods are not based on misleading information-gathering practices.
    d. The Center could not itself legally collect the specific information sought from the individual or information provider, except that the Center may receive aggregated information where:
        i. The individual or information provider has lawfully obtained such information; and
        ii. The Center could lawfully collect the specific pieces of information that comprise the aggregate.
    e. The Center has not taken the steps necessary, such as obtaining a search warrant or subpoena, to be authorized to seek and receive the information.

5. Information gathering and investigative techniques used by the Oregon TITAN Fusion Center will be no more intrusive than is necessary in the particular circumstance to gather information it is authorized to seek or retain under applicable statues and rules.

6. External agencies that access the Oregon TITAN Fusion Center's information or share information with the Center are governed by the laws and rules governing those individual agencies, including applicable federal and state laws.

## 4.3 Classification Regarding Validity and Reliability of Information

1. At the time of retention in a system maintained by the Oregon TITAN Fusion Center, the information will be categorized regarding its:
    a. Content validity;
    b. Nature of the source (anonymous tip, confidential source, trained interviewer or investigator, written statement (victim, witness, other), private sector, or other source); and
    c. Source reliability.

## 4.4 Classification of Information according to limits on access and disclosure

1. At the time a decision is made to retain information, it will be classified pursuant to the applicable limitations on access and sensitivity of disclosure in order to:
    a. Protect an individual's right of privacy and civil rights;
    b. Protect confidential sources and police undercover techniques and methods;
    c. Not interfere with or compromise pending criminal investigations; and
    d. Provide legally required protection based on the status of an individual (such as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter, a domestic violence crime victim or as a witness).

2. At the time a decision is made to retain, or store, criminal intelligence, it will be classified pursuant to the applicable limitations on access and disclosure contained in OAR 137-090-0100. Criminal intelligence information is classified according to the following system: Sensitive, Confidential and Restricted.
   *See,* http://arcweb.sos.state.or.us/rules/OARS 100/OAR 137/137 090.html

3. The classification of stored information will be reevaluated 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.

4. Classifications regarding access will be used to control:
    a. The information to which a particular group or class of users can have access based on the group or class;
    b. What information a class of users may add, change, delete or print; and
    c. To whom the information may be disclosed and under what circumstances.

5. Credentialed, role-based access criteria will be used by the Center, as appropriate, to control:

    a. The information to which a particular group or class of users can have access based on the group or class.
    b. The information a class of users can add, change, delete, or print.

c. To whom, individually, the information can be disclosed and under what circumstances.

6. Access to or disclosure of records retained by the Center will be provided only *to persons within the center 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. 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.

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

## 5.0 Information Quality

The agencies participating in the Oregon TITAN Fusion Center remain the owners of the data they contribute.

Inaccurate personal information can have a damaging impact on the person concerned and on the integrity and functional value of the Center. In order to maintain the integrity of the Oregon TITAN Fusion Center, any agency that obtains information through the Center must independently verify the information with the agency that originally provided it before taking any official action (e.g., warrant or arrest) based on the information.

User agencies and individual users are responsible for complying with applicable laws governing the use, further dissemination, purging, and updating of information obtained from the Center.

**5.1** The Oregon TITAN Fusion Center will make every reasonable effort to ensure that information sought or retained is:

1. Derived from reliable and trustworthy sources of information;

2. Accurate, current; and

3. Complete, including the relevant context in which it was sought or received and other related information; and merged with other information about the same individual or organization only when the applicable standard has been met.

**5.2** The Oregon TITAN Fusion Center will make every reasonable effort to ensure that only authorized users are allowed to add, change, or delete information from criminal intelligence storage systems.

**5.3** The Oregon TITAN Fusion Center will make every reasonable effort to ensure that information will be deleted from criminal intelligence storage systems when the Center learns that:

1. The information is invalid, inaccurate, unverifiable, no longer useful, no longer relevant, or otherwise unreliable;

2. The information does not support a reasonable suspicion of criminal activity;

3. The source of the information did not have authority to gather the information or to provide the information to the Center; or

4. The source of the information used prohibited means to gather the information, except where:
    a. The information was provided through an anonymous tip, in which case the Center may use the information as a basis to investigate further, but shall not retain the information unless it meets the requirements set out in Section 4.1; or
    b. The information was provided by a cooperating defendant or criminal informant and the person was not acting at the direction or under the control of the Center.

**5.4** The Oregon TITAN Fusion Center will investigate, in a timely manner, alleged errors and deficiencies (or refer them to the originating agency) and correct, delete, or refrain from using protected information found to be erroneous or deficient.

**5.5** The Center will conduct periodic data quality reviews of information it originates and make every reasonable effort to ensure that the information will be corrected, deleted from the system, or not used when the Center identifies information that is erroneous, misleading, obsolete, or otherwise unreliable; the Center did not have authority to gather the information or to provide the information to another agency; or the Center used prohibited means to gather the information (except when the Center's information source did not act as the agent of the Center in gathering the information).

**5.6** Originating agencies external to the Center are responsible for reviewing the quality and accuracy of the data provided to the Center. The Center 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.

**5.7** 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]).

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

**5.9** The Oregon TITAN Fusion Center will use written or electronic notification to inform recipient agencies when information previously provided to the recipient agency is deleted or changed by the Center because the information is determined to be

erroneous, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the rights of the individual may be affected.

## 6.0 Collation and Analysis of Information

### 6.1 Collation and Analysis

Information sought or received by the Oregon TITAN Fusion Center or from other sources will only be analyzed:

1. By qualified individuals approved and employed by the Oregon Department of Justice, or by a participating agency, who have successfully completed a background check and appropriate security clearance, if applicable, and have been selected, approved and trained accordingly; and

2. To provide tactical and/or strategic criminal intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal activities generally, including terrorism; or

3. To further crime prevention (including terrorism), law enforcement, public safety, force deployment, or prosecution objectives and priorities established by the Center.

Information sought or received by the agency or from other sources will not be analyzed or combined in a manner or for a purpose that violates Section 4.1.4.

**6.2** Oregon TITAN Fusion Center requires that all analytical products be reviewed and approved by the Privacy Officer to ensure that they provide appropriate privacy, civil rights, and civil liberties protections prior to dissemination or sharing by the Center. Analytical products may be reviewed and approved for dissemination or sharing by the Director of the TITAN Fusion Center, the Oregon Department of Justice - Criminal Justice Division's Special Agent in Charge, Deputy Chief Counsel or the Chief Counsel when:

1. Immediate dissemination or sharing is reasonably necessary to protect life or prevent physical injury where the risk of injury or death is imminent, and

2. The Privacy Officer cannot be contacted or contact with the Privacy Officer would delay dissemination or sharing and delay would reasonably increase the risk of injury or death of a person.

**6.3** Information subject to collation and analysis is information as defined and identified in Section 4.1 1. of this policy.

**6.4** Records about an individual or organization from two or more sources will not be merged by the Oregon TITAN Fusion Center 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 a higher accuracy of match.

**6.5** If the matching requirements are not fully met but there is an identified partial match, the information may be associated by the Oregon TITAN Fusion Center if accompanied by a clear statement that it has not been adequately established that the information relate s to the same individual or organization.

## 7.0 Sharing and disclosure of Information/Criminal Intelligence

This section addresses to whom and under what circumstances the Oregon TITAN Fusion Center may disclose information/criminal intelligence. Disclosure may be passive, by allowing authorized law enforcement personnel access to databases via direct queries, or active, as when the Center disseminates or publishes information in bulletins, notices, or reports.

Information obtained from or through the Oregon TITAN Fusion Center will not be used or disclosed for purposes other than those specified in the Memorandum of Understanding signed by each participating agency. Information cannot be (1) sold, published, exchanged, or disclosed for commercial purposes; (2) disclosed or published without prior approval of the contributing agency; or (3) disseminated to unauthorized persons.

Agencies external to the Oregon TITAN Fusion Center may not disseminate information accessed or disseminated from the Center without approval from the Center or other originator of the information.

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

### 7.1 Sharing Information within the Oregon TITAN Fusion Center and with Other Law Enforcement Agencies

1. Access to information retained by the Oregon TITAN Fusion Center will only be provided to personnel assigned to the Center or in other governmental agencies who are authorized by law to have access; who will use it only for legitimate law enforcement, public protection, public prosecution, or public health purposes (“right to know”); and who will use it only in the performance of their official duties (“need to know”).

2. The Center will maintain an audit trail to document access by or dissemination of information to such persons.

### 7.2 Sharing Criminal Intelligence within the Oregon TITAN Fusion Center and with Criminal Law Enforcement Agencies

Criminal intelligence can only be used for lawful purposes. A lawful purpose means that the request for information is directly linked to a law enforcement agency’s active criminal investigation or is a response to a confirmed lead that requires follow-up to prevent a criminal act.

1. Access to criminal intelligence will be provided according to OAR 137-090-0000 et.seq. and other applicable laws.

2. The Center shall not confirm the existence or nonexistence of criminal intelligence to any person or agency that would not be eligible to receive the information itself.

### 7.3 Sharing Information with those Responsible for Public Protection, Safety, or Public Health

1. Information retained by the Oregon TITAN Fusion Center may be disseminated to individuals in public or private entities only for public protection, safety, or public health purposes ("right to know") and only in the performance of official duties in accordance with applicable laws and procedures ("need to know").

2. An audit trail will be kept of the access by or dissemination of information to such persons.

3. Nothing in this policy shall limit the dissemination, including unsolicited, of an assessment of criminal intelligence information to a government official or to any other individual, when necessary to avoid imminent danger or certain danger to life or property.

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

### 7.4 Sharing Information for Specific Purposes

1. Information gathered and retained by the Oregon TITAN Fusion Center may be disseminated for specific purposes upon request by persons authorized by law to have such access ("right to know") and only for those uses or purposes specified in the law ("need to know").

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

3. 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 for a minimum of 20 years by the Center.

### 7.5 Disclosing Information to the Public

1. Information gathered and retained by the Oregon TITAN Fusion Center may be disclosed to a member of the public only if the information is a public record as defined in ORS 192.410-192.505 and is not exempt from disclosure.

2. The Center may collect a fee from those requesting information, as authorized in ORS 192.440, for costs associated with providing the information.

3. The Oregon TITAN Fusion Center will follow OAR 137-090-0040 in responding to requests for stored criminal intelligence.

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

5. The Center will maintain an audit trail of all requests and of the information disclosed.

## 7.6 Disclosing Information to the Individual about Whom Information has been Gathered

1. Upon satisfactory verification of his or her identity and subject to the conditions specified in Section 7.6.3, an individual is entitled to know the existence of and to review the information about himself or herself that has been gathered and retained by the Center. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information (correction). The Center'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.

2. Upon receiving such a request, the Center will direct the individual to contact the agency that originally submitted the information. The submitting agency will determine what information may be released under the laws governing that agency.

3. The existence, content, and source of the information will not be made available to an individual when:
    a. Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution (ORS 192.501(3));
    b. Disclosure would endanger the health or safety of an individual, organization, or community (ORS 192.501(18) and (23), ORS 192.502(2), (4) and (8));
    c. The information is stored in a criminal intelligence system, such as the Oregon State Intelligence Network (28 CFR Part 23 and ORS 137-090-0150– 137-090-0170); or
    d. Disclosure is otherwise limited or prohibited by law.

4. If the information does not originate with the Center, the request will be referred to the originating agency, if appropriate or required, or the Center will notify the source agency of the request and its determination that disclosure by the Center or referral of the requestor to the source agency was neither required nor appropriate under applicable law.

5. If an individual challenges the accuracy or completeness of information retained at and the Center and for which the Center is the original source, the Center will inform the individual of the procedure for requesting a review of any challenges and for making corrections.
    a. If a request for correction is denied, the Center will advise the individual of the reason(s) for the denial.
    b. The Center will also inform the individual of the procedure for appeal when the Center has declined to correct challenged information to the degree requested by the individual.

c. A record will be kept of all requests for corrections and the resulting action, if any.

6. The agency may collect a fee from those requesting information, as authorized in ORS 192.440, for costs associated with providing the information.

7. The Center will maintain a record of all requests and of the information disclosed to an individual.

8. Information gathered or collected and records retained by the Center 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 disclosure or publication, unless disclosure is agreed to as part of the normal operations of the agency.
    c. Disseminated to persons not authorized to access or use the information.

9. If an individual has a complaint with regard to the accuracy or completeness of terrorism-related protected information that:
    a. Is exempt from disclosure,
    b. Has been or may be shared through the ISE,
        i. Is held by the Oregon TITAN Fusion Center and
        ii. Allegedly has resulted in demonstrable harm to the complainant.

10. The Center will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the Center's Privacy Officer at the following address: 610 Hawthorne Ave, SE, Suite 210, Salem, Oregon, 97301, oregonfusioncenter@doj.state.or.us. The Privacy Officer will acknowledge the complaint and state that it will be reviewed but will not confirm the existence or nonexistence of the information to the complainant unless otherwise required by law. If the information did not originate with the Center, the Privacy Officer will notify the originating agency in writing or electronically within 10 days and, upon request, assist such agency to correct any identified data/record deficiencies, purge the information, or verify that the record is accurate. All information held by the Center that is the subject of a complaint will be reviewed within 30 days and confirmed or corrected/purged if determined to be inaccurate, incomplete, to include incorrectly merged information, or to be out of date. If there is no resolution within 30 days, the Center will not share the information until such time as the complaint has been resolved. A record will be kept by the Center of all complaints and the resulting action taken in response to the complaint.

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

## 7.7 Records that will ordinarily not be provided to the public

1. Records required to be kept confidential by law are exempted from disclosure requirements under ORS 192.410-192.505.

2. Information that meets the definition of "classified information" as that term is defined in the National Security Act, Public Law 235, Section 606 and in accord with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010.

3. Investigatory records of law enforcement agencies that are exempted from disclosure requirements under ORS 192.410-192.505.

4. 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 ORS 192.410-192.505. This includes a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism or an act of agricultural terrorism, vulnerability assessments, risk planning documents, needs assessments, and threat assessments.

5. Protected federal, state, local, or tribal records, which may include records originated and controlled by another agency that cannot, under 28 CFR Part 23 or OAR 137-090-0150 – 137-090-0170 be shared without permission.

6. A violation of an authorized nondisclosure agreement entered into between participating agencies as authorized by Oregon Public Records laws.

# 8.0 Retention, Review, Purge, and Destruction of Information/Stored Criminal Intelligence

## 8.1 Retention and Review of Information

1. When information retained at the Center has no further value or meets the criteria for removal under ORS Chapter 192, OAR 137-090-0000 to 137-090-0225, i28 CFR Part 23, and Center policy, it will be returned to the submitting agency or purged and destroyed according to the above stated law or Center policy.

2. The Director of the ODOJ Criminal Justice Division's Criminal Intelligence Unit or a designee will review information prior to its removal from a record or information storage system.

## 8.2 Destruction of Records Containing Information

1. Records containing information will be destroyed, or returned to the submitting (originating) agency, according to the requirements of OAR 166-300-0015.

2. The Center will provide notification of proposed destruction or return of records to the submitting agency.

3. The Center will maintain a record of the information that has been purged or returned.

### 8.3 Review, Purge, and Destruction of Stored Criminal Intelligence

The Center will follow 28 CFR Part 23 and OAR 137-090-0150 – 137-090-0170 in reviewing, purging, and destroying stored criminal intelligence. The maximum retention period is five (5) years, and a criminal intelligence file must be purged after five years unless the information in that criminal intelligence file has been updated consistent with these Standards and Procedures.

The procedure contained in 28 CFR Part 23 Section D will be followed by Oregon TITAN Fusion Center for notification of appropriate parties, including the originating agency, before information is deleted or returned in accordance with this policy or as otherwise agreed upon with the originating agency in a participation or membership agreement.

1. The Center will maintain a record that information has been purged and destroyed, which will contain at a minimum the date of the purge or return and if returned the name and address of the agency to which it was returned; and for appropriate system(s), notice will be given to the submitter at least 30 days prior to the required review and validation/purge date.

## 9.0 Accountability and Enforcement

### 9.1 Information System Transparency

1. A link to the Oregon TITAN Fusion Center Privacy Policy will be included on the publicly accessible Oregon Department of Justice website, http://www.doj.state.or.us/. The link will be located under "Request for Public Records" and the sub-category "OTFC Privacy Policy."

2. The Oregon TITAN Fusion Center will designate a person who shall be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system. The Privacy Officer may be contacted at 610 Hawthorne Ave, SE, Suite 210, Salem, Oregon, 97301, oregonfusioncenter@doj.state.or.us .

### 9.2 Accountability for Activities

1. ODOJ will appoint a Director for the Center (Center Coordinator) who will have primary responsibility for the day-to-day operation of the Oregon TITAN Fusion Center, including operations, its justice systems; coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing, and disclosure of information; and the enforcement of this Privacy Policy.

2. Use of the Center's information systems is limited to personnel who have been selected, approved, and trained accordingly. Each individual user must complete an Individual User Agreement and is required to abide by this Privacy Policy in the use of information obtained by and through the Center. Individual users remain responsible for their legal and appropriate use of the information contained

therein.

3. The Oregon TITAN Fusion Center's Security Officer is designated and trained to serve as the Center's security officer.

4. The Oregon TITAN Fusion Center will operate in a secure facility protected from external intrusion. Remote access to databases located at the Center's headquarters will be provided over secure network lines.

5. The Center will establish procedures, practices, and system protocols and use software, information technology tools, and physical security measures that protect information from unauthorized access, modification, theft, or sabotage, whether internal or external, and whether due to natural or human-caused disasters or intrusions. The methods and techniques used shall be consistent with security practices that are generally accepted within the law enforcement community.

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

7. The Oregon TITAN Fusion Center will store information in a manner such that it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized by law or agency policy to take such actions.

8. Access to Oregon TITAN Fusion Center information will be granted only to center personnel whose positions and job duties require such access; who have successfully completed a background check and appropriate security clearance, if applicable; and who have been selected, approved, and trained accordingly.

9. Queries made to the Oregon TITAN Fusion Center's data applications will be logged into the data system identifying the user initiating the query.

10. The Oregon TITAN Fusion Center will utilize watch logs to maintain audit trails of requested and disseminated information.

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

12. The Oregon TITAN Fusion Center will adopt and follow procedures and practices to ensure and evaluate the compliance of its users and the system itself with the provisions of this Privacy Policy and applicable law. This will include logging access to these systems and periodic auditing of these systems, so as to not establish a pattern of the audits. These audits will be mandated at least annually and a record of the audits will be maintained by the Privacy Officer or Center Director the Center.

13. The Oregon TITAN Fusion Center will require any individuals authorized to use any system located at the Center's headquarters to provide a written

acknowledgement of receipt of this policy and to agree in writing to comply with the provisions of this Privacy Policy. Such authorized individuals include personnel assigned to the Center and participating users.

14. The Oregon TITAN Fusion Center Executive Advisory Committee internally will annually conduct or coordinate audits and inspections of the information contained in information systems located at the Center's headquarters. The committee has the option of conducting 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 so as to protect the confidentiality, sensitivity, and privacy of the agency's information.

15. The Executive Advisory Committee will also be responsible for overseeing the investigation into any allegation of unauthorized or illegal use of the Center's data or information, including alleged violations of this Policy.

16. The Oregon TITAN Fusion Center Privacy Officer will annually review and update the provisions protecting privacy, civil rights, and civil liberties in its policies and make appropriate changes in response to changes in applicable law and public expectations. This review will be performed with the Center's legal counsel and such other persons as may be designated by the Chief Counsel of ODOJ's Criminal Division.

17. Any changes made to this Policy will be presented to the Oregon TITAN Fusion Center Executive Advisory Committee for approval.

18. The Oregon TITAN Fusion Center will notify an individual about whom unencrypted personal information was or is reasonably believed to have been obtained by an unauthorized person, where such action threatens physical, reputational, or financial harm to the person.

19. The notice will be made promptly and without unreasonable delay following discovery or notification of the unauthorized access, consistent with the legitimate needs of law enforcement to investigate the circumstances surrounding the access or any measures necessary to determine the scope of such access and to reasonably restore the integrity of the information system. Notice need not be given if doing so meets the criteria specified in Section 7.6.3.

20. The audit log of queries made to the Oregon TITAN Fusion Center will identify the user initiating the query.

21. The Oregon TITAN Fusion Center will maintain an audit trail of accessed, requested, or disseminated information. An audit trail will be kept for a minimum of 20 years (pursuant to Oregon Department of Justice Records Retention Schedule and OAR 166-300-0015) of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.
22. The Oregon TITAN Fusion Center's 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.

### 9.3 Enforcement

If a user is suspected of or found to have violated the provisions of this Policy regarding the collection, classification, retention, sharing, use, disclosure, or destruction of information, the Director of the Oregon TITAN Fusion Center will:

1. Suspend or discontinue the user's access to information;

2. Take disciplinary action against the person as permitted by applicable personnel policies;

3. Apply other sanctions or administrative actions as provided in the Center's personnel policies;

4. Request the agency, organization, contractor, or service provider employing the user to initiate proceedings to discipline the user or take other action authorized by the employer's personnel policy; or

5. Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of this Policy as stated in Section 1.
The Oregon TITAN Fusion Center reserves the right to restrict the qualifications and number of personnel having access to Center information and to suspend or withhold service and deny access to any participating agency or participating agency personnel violating the Center's privacy policy.

## 10.0 Training

**10.1** The Oregon TITAN Fusion Center will require the following individuals to participate in training regarding the implementation of and adherence to this Policy:

1. Personnel assigned to the Center;

2. Personnel providing information technology services to the Center;

3. Staff in other public agencies or private contractors providing services to the Center; and

4. Users who are not employed by the Center or a contractor.

**10.2** The Oregon TITAN Fusion Center 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.

**10.3** The Training will cover:

1. The purpose of the Policy;

2. The substance and intent of the provisions of the Policy relating to the collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the Center;

3. The consequences of improper handling or use of information accessible within or through the Center; and

4. Penalties for policy violations, including possible transfer, dismissal, civil and criminal liability, and immunity, if any.

5. Originating and participating agency responsibilities and obligations under applicable law and policy.

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

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

8. Mechanisms for reporting violations of Center privacy protection policies and procedures.

**10.4** Copies of the Policy will be made available in electronic and paper form to all individuals listed in section 10.1 above.

## APPENDIX A
Terms and Definitions

**Access**—Data access is being able to get to (usually having permission to use) particular data on a computer. Web access means having a connection to the World Wide Web through an access provider or an online service provider. Data access is usually specified as read-only and read/write access.

With regard to the ISE, access refers to the business rules, means, and processes by and through which ISE participants obtain terrorism-related information, to include homeland security information, terrorism information, and law enforcement information acquired in the first instance by another ISE participant.

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

**Acquisition**—The means by which an ISE participant obtains information through the exercise of its authorities; for example, through human intelligence collection or from a foreign partner. For the purposes of this definition, acquisition does not refer to the obtaining of information widely available to other ISE participants through, for example, news reports or to the obtaining of information shared with them by another ISE participant who originally acquired the information.

**Agency**—The Oregon TITAN Fusion Center and all agencies that access, contribute, and share information in the Oregon TITAN's justice information system.

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

Audit trails are a fundamental part of computer security, used to trace (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**—The process of validating the credentials of a person, computer process, or device. Authentication requires that the person, process, or device making the request provide a credential that proves it is what or who it says it is. Common forms of credentials are digital certificates, digital signatures, smart cards, biometrics data, and a combination of user names and passwords. See Biometrics.

**Authorization**—The process of granting a person, computer process, or device with access to certain information, services, or functionality. Authorization is derived from the identity of the person, computer process, or device requesting access that is verified through authentication. See Authentication.

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

**Center**—Refers to the Oregon TITAN Fusion Center and all participating state agencies of the Oregon TITAN Fusion Center.

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

**Civil Rights**—The term "civil rights" 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.

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

**Confidentiality**—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**—Consists of information on the activities and associations of:

1. Individuals who:
    a. Based upon reasonable suspicion are suspected of being or having been involved in the actual or attempted planning, organizing, threatening, financing, or commission of criminal acts; or
    b. Based upon reasonable suspicion, are suspected of being or having been involved in criminal activities with known or suspected crime figures.

2. Organizations, businesses, and groups which:
    a. Based upon reasonable suspicion are suspected of being or having been involved in the actual or attempted planning, organizing, threatening, financing, or commission of criminal acts; or

b. Based upon reasonable suspicion are suspected of being or having been illegally operated, controlled, financed, or infiltrated by known or suspected crime figures.
c. Criminal intelligence records are maintained in a criminal intelligence system per 28 CFR Part 23.

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

**Data Breach**—The unintentional release of secure information to an untrusted environment. 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 World Wide Web or on a computer otherwise accessible from the Internet without proper information security precautions; 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, such as unencrypted e-mail; or transfer of such information to the information systems of a possibly hostile agency or environment where it may be exposed to more intensive decryption techniques.

**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 Principles**—The Fair Information Principles (FIPs) are contained within the Organisation for Economic Co-operation and Development's (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. These were developed around commercial transactions and the transborder 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**—Because a privacy notice is not self-implementing, an individual within an organization's structure must also be assigned responsibility for enacting and implementing the notice.

**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, including investigative information; tips and leads data; suspicious activity reports; and criminal intelligence information. Such data may comprise personally identifiable information.

**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.

**Information Sharing Environment (ISE) Suspicious Activity Report (SAR) (ISE-SAR)**—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).

**Intelligence-Led Policing (ILP)**—A process for enhancing law enforcement agency effectiveness toward reducing crimes, protecting community assets, and preparing for responses. ILP provides law enforcement agencies with an organizational framework to gather and use multisource information and intelligence to make timely and targeted strategic, operational, and tactical decisions.

**Invasion of Privacy**—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 constitution, statute, ordinance, regulation, executive order, policy, or court rule, decision, or order as construed by appropriate local, state, or federal officials or agencies.

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

**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**—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**—Applies to all forms of information storage. This includes electronic systems (for example, databases) and nonelectronic 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.

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

**Nonrepudiation**—A technique used to ensure that someone performing an action on a computer cannot falsely deny that he or she performed that action. Nonrepudiation provides undeniable proof that a user took a specific action, such as transferring money, authorizing a purchase, or sending a message.

**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**—Refers to any criminal law enforcement agency that enters into a Memorandum of Understanding with the Oregon TITAN Fusion Center and assigns personnel to work at the Center.

**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 Information or Data**—Personal information refers to any information that relates to an identifiable individual (or data subject). Information that can be used, either alone or in combination with other information, to identify individual subjects suspected of engaging in criminal activity, including terrorism. See also Personally Identifiable Information.

**Personally Identifiable Information**—One or more pieces of information that, when considered together or in the context of how the information is presented or gathered, are sufficient to specify a unique individual. The pieces of information can be:
Personal characteristics (such as height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation, place of birth, mother's maiden name, distinguishing features, and biometrics information, such as fingerprints, DNA, and retinal scans).

A unique set of numbers or characters assigned to a specific individual (including name, address, phone number, social security number, e-mail address, driver's license number, financial account or credit card number and associated PIN number, Integrated Automated Fingerprint Identification System [IAFIS] 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**—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 printed, 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 Center will adhere to those legal requirements and 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 Center, the individual, and the public; and promotes public trust.

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

**Protected Information**—Protected information includes personal data about individuals that is subject to information privacy or other legal protections by law, including the U.S. Constitution and the Oregon constitution; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 23; applicable state and tribal constitutions; and applicable state, local, and tribal laws, ordinances, and codes. Protection may be extended to organizations by fusion Center policy or other state, local, or tribal agency policy or regulation.

**Public—**

1. Public includes:
    a. Any person and any for-profit or nonprofit entity, organization, or association;
    b. Any governmental entity for which there is no existing specific law authorizing access to the agency's information;
    c. Media organizations; and
    d. 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.

2. Public does not include:
    a. Employees of the Oregon TITAN Fusion Center and participating agencies;
    b. People or entities, private or governmental, who assist the Center and participating agencies; and
    c. Public agencies whose authority to access information gathered and retained by the Center is specified in law.

**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**—Laws, policies, and procedures that address public agency responsibilities with regard to access/disclosure and correction of information and the handling of complaints from persons regarding protected information about them which is under the Center's control and which is exempt from disclosure and not disclosed to the individual to whom the information pertains.

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

**Retention**—Refer to Storage.

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

**Right to Privacy**—The 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 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.

**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.

**Source Agency**—Source agency refers to the agency or organizational entity that originates SAR (and when authorized, ISE-SAR) information.

**Storage**—In a computer, storage is the place where data is held in an electromagnetic or optical form for access by a computer processor. There are two general usages:

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 is probably the most common meaning in the IT industry.

In a more formal usage, storage has been divided into (1) primary storage, which holds data in memory (sometimes called random access memory, or RAM) and other "built-in" devices such as the processor's L1 cache, and (2) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations.

Primary storage is much faster to access than secondary storage because of the proximity of the storage to the processor or because of the nature of the storage devices. On the other hand, secondary storage can hold much more data than primary storage.

With regard to the ISE, storage (or retention) refers to the storage and safeguarding of terrorism-related information—including homeland security information, terrorism information, and law enforcement information relating to terrorism or the security of our homeland—by both the originator of the information and any recipient of the information.

**Suspicious Activity**—Defined in the ISE-SAR Functional Standard (Version 1.5) as "observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity." Examples of suspicious activity include surveillance, photography of sensitive infrastructure facilities, site breach or physical intrusion, cyberattacks, testing of security, etc.

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

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

**Terrorism-Related Information**—In accordance with the 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.

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

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

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

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