



Utah Statewide Information & Analysis Center

Information Privacy Policy

Mission Statement

The Statewide Information and Analysis Center (SIAC) is a public safety partnership designed to appropriately collect, analyze, and disseminate intelligence to enhance the protection of Utah's citizens, communities, and critical infrastructure.

I. Purpose

The SIAC Information Privacy Policy ("Privacy Policy") establishes authoritative guidelines and procedures for the roles and responsibilities of SIAC staff and partners, to include users of the criminal intelligence system and other SIAC-maintained technology systems, regarding the manner in which information is sought, collected, handled, stored, retained, archived, accessed, disseminated and purged; and disclosed within the SIAC, as well as with other governmental entities, private entities, and the general public; in order to enforce strict protection of the privacy rights, civil rights, and civil liberties enjoyed by United States citizens under federal and state law.

II. Statutory Authority

The Utah Department of Public Safety is granted statutory authority under Utah Code 53-10-302 to:

- A. Upon request, provide assistance and specialized law enforcement services to local law enforcement agencies [53-10-302 (1)];
- B. Conduct financial investigations regarding suspicious cash transactions, fraud, and money laundering [53-10-302 (2)];
- C. Investigate organized crime, extremist groups, and others promoting violence [53-10-302 (3)];
- D. Investigate criminal activity of terrorist groups [53-10-302 (4)];
- E. Cooperate and exchange information with other (Utah) state agencies and with other law enforcement agencies of government, both within and outside

of the state, to obtain information that may achieve more effective results in the prevention, detection, and control of crime and apprehension of criminals [53-10-302 (6)];

- F. Create and maintain a statewide criminal intelligence system [53-10-302 (7)];
- G. Provide specialized case support and investigate illegal drug production, cultivation, and sales [53-10-302 (8)]; and
- H. Investigate, follow-up, and assist in highway drug interdiction cases [53-10-302 (9)];

III. Policy Applicability and Legal Compliance

This Privacy Policy applies to information about individuals and organizations obtained by the SIAC in furtherance of its analytical mission. In adopting this Privacy Policy, the SIAC shall implement it as an internal operating policy, along with other necessary policies, in a manner consistent with the U.S. Constitution, Utah Code/Constitution, the Intelligence Reform and Terrorism Prevention Act (IRTPA), the Code of Federal Regulations (28 CFR § 23), The Bank Secrecy Act (31 USC § 5311, 31 CFR § 103), and the Utah Government Records Access Management Act (Utah Code Ann. § 63G-2-101 et seq.). The desired outcome of this policy is to enforce strict protection of the privacy rights, civil rights, and civil liberties enjoyed by U.S. citizens under federal and state law.

- A. Information which furthers an administrative or other non-analytical purpose (such as personnel files, or information regarding fiscal, regulatory or other matters associated with the operation of the SIAC as a governmental entity) or which does not identify an individual or organization will be handled in a manner which complies with all applicable privacy laws and regulations but will not be subject to the provisions of this policy.
- B. The SIAC, and all assigned or detailed personnel, shall comply with all laws and regulations that govern the handling of national security classified information. Information that meets the definition of “classified information” is defined in the National Security Act, Public Law 235, Section 606.
- C. All SIAC users including all assigned or detailed personnel, information technology service providers, private contractors, agencies participating in the ISE and other authorized participants in any SIAC operational component (Intelligence Analysis, Intelligence Liaison Officer Program, Critical Infrastructure Protection), shall comply with this Privacy Policy and all applicable laws protecting privacy, civil rights, and civil liberties, including those cited above, in the collection, use, analysis, retention, destruction, sharing, and disclosure of information. The operating policies of each of the SIAC’s operational components will be consistent with this Privacy Policy and will incorporate applicable laws protecting privacy, civil rights, and civil liberties. Violations of this section will be handled as outlined in Section XV Accountability and Enforcement.

- D. All individuals with access to information maintained by SIAC will sign a Non-Disclosure Agreement (NDA).
- E. Participating agencies collocated at the SIAC will sign a Memorandum of Understanding (MOU).
- F. This Privacy Policy will be posted on all SIAC-related web-portals.

IV. Governance and Oversight

- A. The Utah Department of Public Safety has the primary responsibility for the operation of the SIAC, including:
 - 1. Coordination of personnel;
 - 2. The collection, receipt, retention and evaluation of information;
 - 3. The analysis, production, destruction, sharing or disclosure of such information.
- B. Pursuant to the Utah Code Ann. § 53-10-302, the Utah Department of Public Safety shall create and maintain a Statewide Criminal Intelligence System. The Utah Department of Public Safety has established a Governance Board to provide oversight of SIAC operations as described in the SIAC Concept of Operations and SIAC Governance Policy.
 - 1. The Governance Board may recommend the suspension of a participant agency for due cause and recommend, if appropriate, the reinstatement of a suspended participant agency.
 - 2. The Governance Board provides direction to SIAC administration in the development of privacy policy and is responsible for the review and approval of all SIAC policies.
 - The Governance Board will annually and/or randomly direct inspection of records retained within the criminal intelligence system and/or disseminated to determine whether they are in compliance with this policy and with adopted standards and procedures. The Governance Board shall be responsible for ensuring that independent, non-SIAC personnel conduct the audit. The Board shall make an annual report on the audit that will be made available to the public.
 - The Governance Board will hear appeals regarding denials of data-correction complaints when requested.
- C. The SIAC Commander will designate a trained privacy official who is responsible for handling reported errors and violations and, in accordance with specific direction and authorization, will be the focal point for ensuring that the SIAC adheres to this policy and the provisions of the Information Sharing Environment Privacy Guidelines. The SIAC Commander, with the assistance of the SIAC Privacy Official, shall retain responsibility for ensuring that the Privacy Policy is rigorously implemented and reviewed and updated annually.
 - 1. This designation currently belongs to Sergeant Marc Atkinson, a SIAC supervisor, who can be contacted at SIAC@utah.gov or 801.256.2360.

- D. The SIAC Commander, or his or her designee, is responsible for establishing and implementing appropriate procedures for resolving complaints involving suspicious activity report (SAR) information or other matters associated with the handling of information. The Commander, or his or her designee, will be responsible for information systems operations, as well as the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing or disclosure of SAR information. SIAC administration will ensure that best practices and training opportunities are incorporated into its programs as appropriate.

V. Definitions

See Appendix A: Glossary of Terms and Definitions

VI. Information

- A. The primary sources of information to the SIAC are other governmental entities, including other Utah law enforcement agencies and SIAC Intelligence Liaison Officers, and through various information systems operated by governmental entities including searches of publicly available records, particularly those accessible through the Internet).
- B. The SIAC will seek, collect, or retain information (to include placing information in criminal intelligence files) that:
1. ***Is based on a criminal predicate or possible threat to public safety***; or
 2. ***Is based on reasonable suspicion*** that an identifiable individual or organization has committed or is supporting or facilitating 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, Utah, or the nation, and that the information is relevant to the criminal (including terrorist) conduct or activity; or,
 3. 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
 4. Is useful in a crime or threat analysis or in the administration of criminal justice and public safety; or
 5. The source of the information is reliable and verifiable, or limitations on the quality of the information are identified; and
 6. The information was collected in a fair and lawful manner.
 7. Where there is a reasonable likelihood that within one year there will develop a 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, Utah, or the nation and the information is relevant to the criminal (including terrorist) conduct or activity.
- C. The SIAC may retain information that is based on a level of suspicion that is less than "reasonable suspicion", such as tips and leads or suspicious

activity report (SAR) information, subject to the policies and procedures specified in Section (VI.) I. below.

- D. The SIAC **will not** seek or retain, and information-originating agencies will agree not to submit, information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, or sexual orientations. Such information will only be sought, collected and retained if it is:
1. Relevant to whether an individual or organization has engaged in, is engaging in, or is planning criminal (including terrorist) activity; or
 2. Needed by the SIAC or partner agencies:
 - To identify an individual;
 - To operate effectively; or
 - To provide services to the individual or accommodate an individual's religious, ethnic, or cultural requests or obligations.
- E. The SIAC will apply labels to agency-originated information in accordance with the policies and procedures specified in this Section (VI.), as well as in Section VIII. Information which pertains to U.S. Persons or is subject to specific restrictions on access, use or disclosure will be marked appropriately.
- F. SIAC personnel will, upon receipt of information, assess the information to determine its nature, usability, and quality. Personnel will assign categories to the information (or ensure that the originating agency will assign categories to the information) to reflect the assessment, such as:
1. Whether the information consists of tips and leads data, suspicious activity report (SAR) information, criminal history, intelligence information, case records, conditions of supervision, case progress, or Protected Critical Infrastructure Information (PCII), etc.;
 2. The nature of the source as it affects veracity (e.g., anonymous tip, trained interviewer or investigator, public record, private sector, etc.);
 3. The reliability of the source (i.e., reliable, usually reliable, unreliable, unknown);
 4. The validity of the content (i.e., confirmed, probable, doubtful, cannot be judged);
 5. The completeness of the information provided; and
 6. The relevance and timeliness of the information, in regards to the date its accuracy was last verified, as well as whether or not the information is still applicable.
 7. The categorization of retained information may be reevaluated when new information is gathered that has an impact on the validity and reliability of retained information.
 8. Categorization requirements do not apply to analytical products and other information obtained from or originated by a federal, state or local entity that has itself evaluated the validity and reliability of information in accordance with these principles or the conventions of the intelligence and law enforcement communities.

- G. At the time a decision is made to retain information, it will be labeled, to the maximum extent feasible, pursuant to applicable limitations on access and sensitivity of disclosure to:
1. Protect confidential sources and police undercover techniques and methods;
 2. Not interfere with or compromise pending criminal investigations;
 3. Protect an individual's right of privacy, civil rights and civil liberties; and
 4. Provide legally required protection based on the status of an individual as a victim or witness, 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.
- H. The classification of existing information will be reevaluated whenever:
1. New information is added that has an impact on access limitations or the sensitivity of disclosure of the information; or
 2. There is a change in the use of the information affecting access or disclosure limitations (e.g., the information becomes part of court proceedings for which there are different public access laws).
- I. SIAC 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***. SIAC personnel will:
1. 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 reliability of the information have been unsuccessful.
 2. 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 distinguish it from other information.
 3. Allow access to or disseminate the information using the same (or a more restrictive) access or dissemination method that is used for data that rises to the level of reasonable suspicion (e.g., "need-to-know" and "right-to-know" access or dissemination).
 4. 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.
 5. Retain information long enough to work a tip or lead or SAR information (maximum of one year before retention review – see Section XIV., H.; mandatory supervisor review every 90 days) to determine its credibility and value, assign a "disposition" label (for example, undetermined or unresolved, cleared or unfounded, or under active investigation) so that a subsequently authorized user knows that status and purpose for the

retention and will retain the information based on the retention period associated with the disposition label.

6. Adhere to and follow the SIAC's physical, administrative, and technical security measures that are in place for the protection and security of tips and leads information. Tips, leads, and suspicious activity reports will be secured in a system that is the same or similar to the system that secures data that rises to the level of reasonable suspicion.
 7. If the information collected in the course of determining reasonable suspicion/criminal predicate was derived from Tips, Leads, and/or SAR information, the information may be retained in a system external to the SIAC intelligence system if, at a minimum, all personally identifiable information (or privacy field information) is removed and purged.
 8. Unless otherwise indicated by the source or submitting agency, source reliability is deemed to be "unknown" and content validity "cannot be judged." In such case, users must independently confirm source reliability and content validity with the source or submitting agency or validate it through their own investigation.
 9. Notify the source agency of the disposition of the SAR information.
- J. The SIAC will incorporate the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious activities and incidents (SAR process) into existing processes and systems used to manage other crime-related information and criminal intelligence, thus leveraging existing policies and protocols utilized to protect the information, as well as constitutional rights, including personal privacy and other civil rights and civil liberties.
- K. The SIAC will identify and review protected information that originated in the SIAC prior to sharing that information in the Information Sharing Environment (ISE). Further, the SIAC will provide notice mechanisms, including but not limited to metadata or data fields, that will enable ISE authorized users to determine the nature of the protected information and how to handle the information in accordance with applicable legal requirements.
1. The SIAC will ensure that SAR information posted in an external repository that is not verified (confirmed) will be subject to continuing assessment for confidence by subjecting it to an evaluation or screening process to confirm its credibility and value or categorize the information as unfounded or uncorroborated. Information determined to be unfounded will be purged from the Information Sharing Environment (ISE) shared space.
 2. Due diligence will be exercised in determining source reliability and content validity.
- L. The SIAC requires certain basic descriptive information to be entered and electronically associated with data (or content) that is to be accessed, used, and disclosed, including:
1. The name of the originating department, component, and subcomponent.
 2. The name of the agency's justice information system from which the information is disseminated.
 3. The date the information was collected, and where feasible, the date its accuracy was last verified.

4. The title and contact information for the person to who questions regarding the information should be directed.
 5. Articulation of reasonable suspicion/criminal predicate for collecting and retaining the information.
- M. The SIAC 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.
- N. The SIAC shall keep a record of the source of information retained by the Center. In this context, "source" refers to the individual or entity which provided the information to the SIAC. If the source is an agency, governmental entity, or other organization, such as a corporation or association, this requirement can be met by maintaining the name of the agency, governmental entity, or organization, as long as the specific unit of that agency, governmental entity, or organization which provided the information is identified.
- O. Non-Criminal information may be filed and retained **only** if the information:
1. Is relevant to the identification of a criminal suspect or to the criminal activity in which the suspect is engaged. The individual or organization which is the criminal suspect identified by this information otherwise meets all requirements of 28CFR Part 23.
 2. Is labeled as "Non-Criminal Identifying Information". It is imperative that, where it is determined to be necessary to support authorized analytical or investigative activity, non-criminal identifying information be clearly labeled as such to ensure that the subject of the information is not inappropriately connected to criminal activity.
 3. Identifying information may not be used as an independent basis to meet the requirement of reasonable suspicion of involvement in criminal (including terrorist) activity.
- P. A SIAC supervisor shall review all information and approve or deny its retention within a SIAC intelligence system based upon the following:
- a. The information meets all requirements of this privacy policy; and
 - b. The source clearly defined reasonable suspicion/criminal predicate for the collection and retention of the information.
- Q. SIAC personnel are required to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of **Critical Infrastructure Information (CII)**. SIAC personnel will:
- a. Maintain compliance with the Homeland Security Act of 2002;
 - b. Maintain compliance with the Critical Infrastructure Information Act of 2002;
 - c. Maintain compliance with the Protected Critical Infrastructure Information (PCII) Program;
 - d. Label data as PCII when it meets the criteria of the PCII program; and

- e. As specified in Section XI., comply with the Utah Government Records Access Management Act (GRAMA), and/or applicable provisions of federal laws, regulations, and executive orders that govern the disclosure of classified or sensitive but unclassified information, in regards to the disclosure of CII outside the SIAC.
- f. Store all CII data in a secure repository separate from all other SIAC data.
- g. The SIAC Critical Infrastructure Protection Coordinator, as well as all other SIAC personnel that work with CII, will be trained and certified in the Protected Critical Infrastructure Information Program (PCII).

VII. Acquiring and Receiving Information

- A. Information gathering (acquisition and access) and investigative techniques used by the SIAC and information-originating agencies shall be in compliance with, and will adhere to, applicable regulations and guidelines, including, but not limited to:
 - 1. 28 CFR Part 23 regarding criminal intelligence information;
 - 2. Organisation for Economic Co-operation and Development's (OECD) Fair Information Practices (under certain circumstances, there may be exceptions to the Fair Information Practices, based, for example, on authorities paralleling those provided in the federal Privacy Act; state, local, and tribal laws; or SIAC policy);
 - 3. Applicable criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) National Criminal Intelligence Sharing Plan (NCISP);
 - 4. Best practices advised by Law Enforcement Intelligence Unit (LEIU) and International Association of Law Enforcement Intelligence Analysts (IALEIA); and
 - 5. Applicable constitutional provisions, Utah code, and the applicable administrative rules, as well as any other regulations that apply to multijurisdictional intelligence databases (See Sections II. and III.).
- B. The SIAC'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 SIAC staff will be trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism.
- C. The SIAC's SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved in activities that have been determined to be consistent with criminal activities associated with terrorism will be documented and shared through the ISE. These safeguards are intended to ensure that information that could violate civil rights and civil liberties (e.g., race, culture, religion, or political associations) will not be intentionally or inadvertently gathered, documented, processed, and shared.
- D. Information gathering and investigative techniques used by the SIAC will (and for originating agencies should) be the least intrusive means necessary

in the particular circumstances to gather information it is authorized to seek or retain.

- E. External agencies that access and share information with the SIAC are governed by the laws and rules governing those individual agencies, as well as by applicable federal and state laws.
- F. The SIAC will contract only with commercial database entities that demonstrate that their methods for gathering personally identifiable information comply with applicable local, state, tribal, territorial, and federal laws, statutes, and regulations and that these methods are not based on misleading information collection practices.
- G. The SIAC will not directly or indirectly receive, seek, accept, or retain information from:
 - 1. An individual or nongovernment information provider if the SIAC knows or has reason to believe that the individual or information provider is legally prohibited from obtaining the specific information sought or disclosing it to the SIAC.
 - 2. An individual or nongovernmental entity who may or may not receive a fee or benefit for providing the information
- H. The SIAC will maintain a record of all information sought and received.
- I. While the participant organizations of the SIAC may have criminal investigative responsibilities, the SIAC will not have lead authority or lead responsibility in criminal investigations.

VIII. Information Quality Assurance

A substantial portion of the information received by the SIAC is in the form of completed analytical product. The SIAC will use these products to assist investigations, support prosecutions, and in furtherance of its mission to analyze and assess strategic threats to the state. SIAC partners may use the information in furtherance of investigative or other activities within their jurisdiction and authority.

- A. The rigorous examination of information quality is a critical component of effective analysis. Thus, the SIAC will make every reasonable effort to ensure that information sought or retained is:
 - 1. Derived from dependable and trustworthy sources of information;
 - 2. Accurate;
 - 3. Current/Relevant;
 - 4. Complete; and
 - 5. Merged with other information about the same individual or organization only when the applicable standard has been met (see Section X.).
- B. Prior to the time of retention in the system, the information will be labeled regarding its level of quality (accuracy, completeness, currency, and confidence (verifiable and reliable)) by the submitting participant.

- C. All SIAC personnel will be trained to appropriately review all information to ensure its suitability and approve or deny its retention prior to the information being retained within any SIAC system based upon clearly defined reasonable suspicion/criminal predicate, as well as all other guidance directed through this Privacy Policy. A SIAC supervisor will be responsible for approving or denying the retention of information within a SIAC intelligence system.
- D. The SIAC will make every reasonable effort to ensure that only authorized users are allowed to add, change, or delete information in the system.
- E. The labeling of retained information will be reevaluated when new information is gathered that has an impact on the SIAC's confidence in the validity or reliability of retained information
- F. The SIAC will actively research suspected errors and deficiencies and will make every reasonable effort to ensure that information will be corrected or deleted from the system when:
 - 1. The information is erroneous, misleading, obsolete, or otherwise unreliable;
 - 2. The source of the information did not have authority to gather the information or to provide the information to the SIAC; or
 - 3. The source of the information used prohibited means to gather the information, except when the source did not act as an agent to a bona fide law enforcement officer.
- G. Originating agencies providing data remain the owners of the data contributed. The SIAC will take reasonable steps to advise the appropriate data owner if its data is found to be inaccurate or incomplete where the SIAC is the primary or initial recipient of such information.
- H. The SIAC shall take reasonable steps to ensure that all records are accurate, relevant, timely, and complete. Such standards must be met when records are used to make any determination about an individual. When SIAC personnel transfer a record outside of the SIAC, the SIAC shall correct, update, withhold, or delete any portion of the record that it knows or has reason to believe is inaccurate or untimely. The SIAC shall notify recipient agencies if information provided by the SIAC is determined to be inaccurate, incomplete, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the rights of the subject individual may be affected.

IX. Collation and Analysis of Information

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

- B. Information subject to collation and analysis is information as defined and identified in Section VI.
- C. Information acquired or received by the SIAC or accessed from other sources is analyzed according to priorities and needs, and will be analyzed only to:
 - 1. Further crime prevention (including terrorism), enforcement, force deployment, or prosecution objectives and priorities established by the SIAC and partner agencies.
 - 2. 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.
 - 3. Provide threat and risk assessments from which local, state, and federal agency leadership can base decisions (i.e., enhance/reduce security postures, prioritize and allocate resources, and increase awareness).

X. Merging of Records/Information from Different Sources

- A. The set of personal identifying information sufficient to allow merging will utilize reasonable steps to identify the subject and may include the name (full or partial) and, in most cases, one or more of the following: date of birth; law enforcement or corrections system identification number; individual identifiers, such as fingerprints, photographs, physical description, height, weight, eye and hair color, race, ethnicity, tattoos, or scars; social security number; driver's license number; or other biometrics, such as DNA, retinal scan, or facial recognition. The identifiers or characteristics that, when combined, could clearly establish that the information from multiple records is about the same organization may include the name, federal or state tax ID number, office address, and telephone number.
- B. If the matching requirements are not fully met but there is a strong partial match, the information may be associated ***if accompanied by a clear statement*** that it has not been completely established that the information relates to the same individual or organization.

XI. Information Sharing, Dissemination, and Disclosure

- A. Credentialed, role-based access criteria will be used, as appropriate, to control:
 - 1. The information to which a particular group or class of users can have access based on the group or class;
 - 2. The information a class of users can add, change, delete, or print; and
 - 3. To whom, individually, the information can be disclosed and under what circumstances.
- B. Access to or disclosure of records retained by the SIAC will be provided ***only to persons within the SIAC or in other governmental agencies*** who are authorized to have access and have a legitimate law enforcement, public protection, public prosecution, public health or justice purpose pursuant to Utah Code Ann. § 63G-2-206. Additionally, such disclosure or access shall only be granted for the performance of official duties in accordance with law

and procedures applicable to the agency for which the person is employed. An audit trail will be kept of access by or dissemination of information to such persons.

- C. Records retained by the SIAC may be accessed or disseminated ***to those responsible for public protection, safety, or public health*** only for public protection, safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures. An audit trail will be kept of access by or dissemination of information to such persons.
- D. Information gathered and records retained by the SIAC may be accessed or disseminated ***for specific purposes*** upon request by persons authorized by law to have such access and only for those users and purposes specified in the law. An audit trail will be kept for a minimum of five years of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.
- E. Criminal intelligence information may be disseminated to law enforcement, homeland security, or counterterrorism agencies for any type of detective, investigative, preventive, or intelligence activity when the information falls within the law enforcement, counterterrorism, or national security responsibility of the receiving agency; or, may assist in preventing a crime or the use of violence, or any conduct dangerous to human life or property; or, to officials within the U.S. Department of Justice Office of Justice Programs when they are monitoring or auditing the SIAC's compliance with 28 CFR Part 23. Participating agencies that access information from the SIAC must comply with all applicable dissemination limitations or practices imposed by the SIAC or the originator of the information. An audit trail will be kept of the access by or dissemination of information to such persons.
- F. The employees and users of the participating agencies and of the SIAC's information service providers will comply with all applicable laws protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing, and disclosure of information. The SIAC will include the statement provided below in all transmittal documents when information is disseminated:

"Receipt of this information constitutes acceptance of all terms and conditions regarding its use, handling, storage, further dissemination or destruction. At a minimum, recipient acknowledges a commitment to comply with all applicable laws protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing and disclosure of information."

- G. All disseminated SIAC intelligence/information products will contain, at a minimum, the following handling notice:

“Recipients are reminded that Utah Statewide Information and Analysis Center intelligence products may contain sensitive information meant for use primarily within the law enforcement and homeland security communities. Such products shall not be released in either written or oral form to the media, the general public, or other personnel who do not have a valid need-to-know without prior approval from an authorized Statewide Information and Analysis Center official. Unlawful dissemination of this information may adversely impact ongoing investigations, disclose protected witness identities and/or collection methods, and thereby compromise law enforcement officers’ safety and the safety and welfare of the public.”

- H. Agencies external to the SIAC may not disseminate information received from the SIAC without specific approval of the originator of the information, and will be subject to the same restrictions on access as provided in Utah Code Ann. § 63G-2-206, unless directed otherwise.
- I. The SIAC adheres to national standards for the 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 Functional Standard for suspicious activity reporting.
- J. The SIAC routinely receive tips, leads, or other reports of suspicious activities. SIAC personnel evaluate the information and, where appropriate, forward it to partner agencies in accordance with applicable procedures and direction provided by SIAC policy and procedures. Depending on the nature of the information, and particularly when credible information indicates a potential danger to life and property, the SIAC may report the information to the appropriate division/bureau within the Department of Public Safety; the Federal Bureau of Investigations; the Department of Homeland Security; and other local, state, and federal government entities with law enforcement or national security responsibilities.
- K. SAR information submitted into an external SAR repository such as ISE-SAR or e-Guardian and retained by the SIAC will be accessed by or disseminated only to persons within the SIAC or, as expressly approved by the appropriate authority for the applicable SAR repository, to include users of the system who are authorized to have access and need the information for specific purposes authorized by law. Access and disclosure of personal information will only be allowed to agencies and individual users that comply with the principles set forth in 28 CFR Part 23, need access to the information for legitimate law enforcement and public protection purposes, and will use the information only for the performance of official duties in accordance with law.
- L. Information gathered and records retained by the SIAC will not be:
 - 1. Sold, published, exchanged, or disclosed for commercial purposes;

2. Disclosed or published without prior notice to the contributing agency that such information is subject to re-disclosure or publication; or
 3. Disseminated to unauthorized persons.
- M. Information gathered and records retained by the SIAC may be accessed or disclosed ***to a member of the public ONLY*** if the information is defined by Utah Code to be public record or otherwise appropriate for release to further the SIAC mission and is not exempt from disclosure by law. Such information may be disclosed only in accordance with the law and procedures applicable to the SIAC for this type of information or when there is a legitimate need. An audit trail will be kept of all requests and of what information is disclosed to a member of the public
- N. Information will be disclosed to a member of the public who requests such information unless the disclosure of such information is exempt from disclosure by the Utah Government Records Access Management Act (GRAMA) or applicable provisions of federal laws, regulations, and executive orders, which govern the disclosure of classified or sensitive but unclassified information.
- O. Public records required to be kept confidential by law are exempted from disclosure requirements under the Critical Infrastructure Information Act of 2002, among other provisions of law.
- P. There are several categories of records that will ordinarily not be provided to the public:
1. Criminal investigative information and criminal intelligence information. These records are classified as protected under Utah Code Ann. § 63G-2-305(9) through (12).
 2. Information that is constitutionally protected from disclosure (i.e., information in which there is an individual privacy interest that clearly exceeds the merits of public disclosure, and matters related to individual or public safety).
 3. Threat, vulnerability, and risk assessments and event/situation planning documents. Utah Code Ann. § 63G-2-106 protects records of a governmental entity or political subdivision regarding security measures designed for the protection of persons or property, public or private. These records are not subject to the Utah Government Records Access Management Act.
 4. Proprietary data/information submitted by government, public, and private sector partners related to critical infrastructure that falls within the definition of Protected Critical Infrastructure Information (PCII).
- Q. A record or part of a record the public disclosure of which would have a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack is exempted from disclosure requirements under various sections of the Utah Code, including but not limited to Utah Code Ann. § 63G-2-305. This includes a record, vulnerability assessment, risk planning document, needs assessment, or threat assessment assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism.

- R. Pursuant to Utah Code Ann. § 63G-2-305 the following records are protected from public disclosure:
- a. Records created or maintained for civil, criminal, or administrative enforcement purposes or audit purposes, or for discipline, licensing, certification, or registration purposes, if release of the records:
 - Reasonably could be expected to interfere with investigations undertaken for enforcement, discipline, licensing, certification, or registration purposes; or
 - Reasonably could be expected to interfere with audits, disciplinary, or enforcement proceedings; or
 - Would create a danger of depriving a person of a right to a fair trial or impartial hearing; or
 - Reasonably could be expected to disclose the identity of a source who is not generally known outside of government and, in the case of a record compiled in the course of an investigation, disclose information furnished by a source not generally known outside of government if disclosure would compromise the source; or
 - Reasonably could be expected to disclose investigative or audit techniques, procedures, policies, or orders not generally known outside of government if disclosure would interfere with enforcement or audit efforts.
 - b. Records the disclosure of which would jeopardize the life or safety of an individual.
 - c. Records the disclosure of which would jeopardize the security of governmental property, governmental programs, or governmental recordkeeping systems from damage, theft, or other appropriation or use contrary to law or public policy.
 - d. Records that, if disclosed, would jeopardize the security or safety of a correctional facility, or records relating to incarceration, treatment, probation, or parole, that would interfere with the control and supervision of an offender's incarceration, treatment, probation, or parole.
 - e. Records provided by the United States or by a government entity outside the state that are given to the governmental entity with a requirement that they be managed as protected records if the providing entity certifies that the record would not be subject to public disclosure if retained by it.
 - f. Records that provide detail as to the location of an explosive, including a map or other document that indicates the location of:
 - a production facility; or
 - a magazine.
 - g. Records related to an emergency plan or program prepared or maintained by the Division of Homeland Security the disclosure of which would jeopardize:
 - the safety of the general public; or
 - the security of: governmental property; governmental programs; or the property of a private person who provides the Division of Homeland Security information.

- S. The SIAC will comply with court orders for dissemination issued in compliance with Utah Code Annotated § 63G-2-207. Records of all such orders and information disclosed shall be kept.
- T. The SIAC shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.
- U. 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 danger to life or property. An audit trail will be kept of the access by or dissemination of information to such persons.

XII. Redress Disclosure

- A. Upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity and subject to the conditions specified in B., below, an individual is entitled to know the existence of and to review the information about him or her that has been gathered and retained by the SIAC. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information. The SIAC's response to the request for information will be made within a reasonable time and in a form that is readily intelligible to the individual. A record will be kept of all requests and of what information is disclosed to an individual.
- B. If an individual requests information about him or her ***that originates with another agency***, the SIAC Privacy Official will notify the individual and the source agency of the request.
- C. To the extent information is maintained in information systems controlled by the State of Utah, the SIAC will comply with the Utah Government Records Access Management Act and other applicable laws and regulations governing the disclosure of information to the individual about whom information has been gathered. To the extent consistent with these laws and regulations, the existence, content, and source of the information will not be made available to an individual when:
 - 1. Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution;
 - 2. Disclosure would endanger the health or safety of an individual, organization, or community;
 - 3. The information is in a criminal intelligence system;
 - 4. The information source does not reside with the SIAC; or
 - 5. The SIAC did not originate, or does not otherwise have a right to disclose, the information.

Complaints and Corrections

- A. If an individual has complaints or objections to the accuracy or completeness of information retained about him or her ***originating with the SIAC***, the SIAC Privacy Official, Sergeant Marc Atkinson, will inform the individual of the procedure for submitting complaints or requesting corrections, by mail, e-mail, or in person. A SIAC complaint/correction form request shall be used to document the request. A record will be kept of all complaints and requests for corrections, the responsive action taken, if any, and a brief explanation of the rationale. An initial response to a complaint or request for correction must be made within ten (10) working days of receipt of the complaint or request.
1. The request will document the individual's understanding of the record, the basis for his/her belief that the record is inaccurate, and the nature of the relief requested. The request should include all appropriate documentation.
 2. Upon receipt of a complaint or request for correction, the SIAC Privacy Official will consent to the correction, remove the record, or state in writing a basis for the denial of the complaint or request.
 3. All denials will be reviewed and approved by the SIAC Commander.
- B. If an individual has complaints or objections to the accuracy or completeness of information about him or her ***that originates with another agency***, the SIAC Privacy Official will notify the source agency of the complaint or correction request and coordinate with the source agency to ensure that the individual is provided with applicable complaint submission or correction procedures. SIAC personnel will make all reasonable efforts to assist agencies in resolving complaints and/or making corrections. A record will be kept of all complaints and correction requests, regardless of the originating agency, and the resulting action taken, if any.
- C. If an individual has a complaint or objection to the accuracy or completeness of terrorism-related information that has been or may be shared through the ISE that: (a) is held by the SIAC; (b) allegedly resulted in harm to the complainant; and (c) is exempt from disclosure, the SIAC will inform the individual of the procedure for submitting (if needed) and resolving complaints or objections. Complaints should be addressed to Sergeant Marc Atkinson at SIAC, 410 West 9800 South, Sandy, Utah 84070 or SIAC@utah.gov. . The SIAC will acknowledge the complaint and state that it will be reviewed, but will not confirm the existence of the information that is exempt from disclosure, unless otherwise required by law. If the information did not originate with the SIAC, SIAC will notify the originating agency in writing and, upon request, assist such agency to correct or purge any identified data/record deficiencies or to verify that the record is accurate. Any personal information originating with the SIAC will be reviewed within 30 days and confirmed or corrected in or deleted from SIAC data/records if it is determined to be erroneous, include incorrectly merged information, or out of date. If there is no resolution within 30 days, the SIAC will not share the information until such time as the complaint has been resolved. A record will be kept of all complaints or requests for corrections and the resulting action, if any.

- D. To delineate protected information shared through the ISE from other data, the SIAC maintains records of the ISE participating agencies to which the center has access, as well as audit logs, and employs system mechanisms whereby the source (or originating agency, including ISE participating agencies) is identified within the information.
- E. The individual to whom information has been disclosed will be given reasons if requests for correction(s) are denied by the SIAC, originating agency, or the ISE participating agency. The individual will also be informed of the procedure for appeal when the SIAC, originating agency, or ISE participating agency has declined to correct challenged information to the satisfaction of the individual to whom the information relates.
- F. The existence, content, and source of the information will not be made available when – consistent with Sections XI. and XII.– disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution; disclosure would endanger the health or safety of an individual, organization, or community; or the information is in a criminal intelligence system.
- G. Unless the requested relief is granted, a final response must provide a brief discussion of the basis for a decision to deny the requested relief as well as information about the process of obtaining further review, reconsideration or appeal from the initial determination. The appellate authority belongs to the SIAC Governance Board.

XIII. Security Safeguards

- A. A SIAC Supervisor will be designated and trained to serve as the SIAC Security Officer. This designation currently belongs to the SIAC's Sgt. (Supervisor).
- B. The SIAC will operate in a secure facility protecting the facility from external intrusion. The SIAC will utilize secure internal and external safeguards against network intrusions. Access to SIAC databases from outside the facility will only be allowed over secure networks.
 - 1. Access to the SIAC can only be granted by designated SIAC personnel. Law Enforcement credentials, and/or a valid state drivers license must be displayed and verified by SIAC management to gain access for both escorted and un-escorted access. A record/log will be maintained of all SIAC visitors that are not granted unescorted access.
 - 2. Two-factor authentication – to include biometric data – is required for un-escorted access to the SIAC facility.
- C. The SIAC will secure tips, leads, and SAR information in a separate repository system that is the same as or similar to the system that secures data rising to the level of reasonable suspicion.

- D. The SIAC will store information in a manner such that it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions.
- E. Access to SIAC information will only be granted to SIAC personnel and partners whose position and job duties require such access; who have successfully completed a background check and appropriate security clearance, if applicable, and have been selected, approved, and trained accordingly.
- F. Queries made to SIAC data applications will be logged into each respective data system identifying the user initiating the query, as well as the date and time of the query whenever possible.
- G. The SIAC will utilize record logs to maintain records of requested, sought and collected, and disseminated information.
- H. To prevent inadvertent public records disclosure, risk and vulnerability assessments will not be stored with publicly available data.
- I. Violations of this policy or internal operating policies at the SIAC will be reported to the SIAC Commander or his or her designee.

XIV. Information Retention and Destruction

- A. All information other than analytical product will be reviewed for record retention (validation or purge) at least every five (5) years, as provided by 28 CFR Part 23. Information may be reviewed through automated or other means. Records need not be individually examined to comply with this requirement when purging. The date and means of review will be documented.
- B. When information has no further value or meets criteria for removal according to this Privacy Policy or according to applicable law, it will be purged, destroyed, deleted, or returned to the submitting source.
- C. The SIAC will delete information or return it to the source, unless it is validated as specified in 28 CFR Part 23.
- D. Records retained by SIAC will comply with Utah Code Ann. § 63G-2-604 when applicable. The SIAC will submit to the State Records Committee a proposed schedule for the retention and disposition of each type of material that is defined as a record pursuant to GRAMA.
- E. Permission to destroy or return information or records will be presumed if the applicable information is not validated within the specified time period, as per item C. above.

- F. Notification of proposed destruction or return of records may or may not be provided to the contributor, depending on the relevance of the information and any agreement with the providing agency.
- G. A record of information to be reviewed for retention will be maintained by the SIAC, 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.
- H. **All SAR information** will be reviewed for retention annually. At the end of one year, SAR information must be either purged or converted into criminal intelligence files, if the information satisfies the requirements for submission into criminal intelligence files. SAR information may be retained if, at a minimum, all personally identifiable information (or privacy field information) is removed and purged.

**XV. Accountability and Enforcement
Information System Transparency:**

- A. The SIAC will be open with the public in regard to information and intelligence collection practices. This Information Privacy Policy will be made available to the public on request and through any public web sites providing information about the SIAC.
- B. The SIAC's Privacy Official will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the SIAC's information systems

Accountability for Activities:

- A. Primary responsibility for the operation of the SIAC information systems—including operations; coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing, and disclosure of information; and the enforcement of this policy—will be assigned in writing to a specific individual. This responsibility currently resides with the SIAC Commander.
- B. The SIAC will protect information from unauthorized access, modification, theft, or sabotage, whether internal or external and whether due to natural or human-caused disasters or intrusions.
- C. The SIAC will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with their systems, in provisions of this policy and applicable law. This will include logging access of these systems and periodic auditing of these systems, so as to not establish a pattern of the audits. A record of the audit will be maintained by the Commander (or designee) of the Center.
 - 1. Queries made to the SIAC data applications will be logged into each respective data system identifying the user initiating the query, as well as the date and time of the query when possible.

2. The SIAC will maintain an audit trail of accessed, requested, or disseminated information. An audit trail will be kept for a minimum of five (5) years of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.
- D. The SIAC will require any individuals authorized to use the system to agree in writing to comply with the provisions of this policy. The SIAC will provide a printed and/or electronic copy of this policy to all SIAC and non-SIAC personnel who provide services and will require of both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and the provisions it contains.
- E. At the direction of the SIAC Governance Board, independent, non-SIAC personnel will conduct audits and inspections of the information contained in its criminal intelligence system at least once per year. All audits will be conducted in a manner that protects the confidentiality, sensitivity, and privacy of the SIAC's criminal intelligence system.
- F. SIAC management may order periodic, internal audits of its information systems to ensure compliance with this privacy policy.
- G. The SIAC, in consultation with the SIAC Governance Board and the DPS Legal Advisor, will periodically review and update the provisions protecting privacy, civil rights, and civil liberties in this policy and make appropriate changes in response to changes in applicable law, technology, the purpose and use of the information systems, and public expectations.
- H. The SIAC's personnel or other authorized users shall report violations, or suspected violations, of SIAC policies relating to protected information to the SIAC's Privacy Official and/or the SIAC Commander.

Inadvertent Disclosure:

- A. The SIAC will notify an individual about whom personal information was or is reasonably believed to have been breached or obtained by an unauthorized person and access to which threatens physical, reputational, or financial harm to the person. The notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement, as provided in subdivision (C) below, and to investigate the release or any measures necessary to determine the scope of the release of information and, if necessary, to reasonably restore the integrity of any information system affected by this release.
- B. With regard to computerized data that includes personal information that the SIAC does not own, SIAC personnel shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

- C. The notification required by this section may be delayed if the SIAC or other law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.
- D. For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the SIAC. Good faith acquisition of personal information by an employee or partner of the SIAC for the purposes of the SIAC mission is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.
- E. For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
 - 1. Social security number;
 - 2. Driver's license number or Utah Identification Card number;
 - 3. Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account;
 - 4. Medical information; or
 - 5. Health insurance information.
- F. For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
- G. For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.
- H. For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.
- I. For purposes of this section, "notice" may be provided by one of the following methods:
 - 1. Written notice;
 - 2. Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code; or
 - 3. Substitute notice, if the cost of providing notice is deemed "excessive", or the SIAC does not have sufficient contact information. Substitute notice shall consist of all of the following:

- E-mail notice when the SIAC has an e-mail address for the subject person(s);
- Conspicuous posting of the notice on the SIAC's web site; or
- Notification to major statewide media.

Enforcement:

- A. If a user is suspected of or found to be in noncompliance with the provisions of this policy regarding the collection, use, retention, destruction, sharing, classification, or disclosure of information, the SIAC will take appropriate action based on the facts and circumstances of the specific incident. These include the following:
1. Suspend or discontinue access to information by the user;
 2. Suspend, demote, transfer, or terminate the person as permitted by applicable personnel policies;
 3. Apply other sanctions or administrative actions as provided by DPS rules and regulations or as provided in SIAC personnel policies;
 4. If the user is from an agency external to the SIAC, request that the relevant agency, organization, contractor or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions; or
 5. Refer the matter to appropriate authorities for criminal prosecution, as necessary and appropriate, to effectuate the purposes of this policy.
 6. Participating employees of the SIAC who perform an act forbidden by law may be charged with official misconduct, under Utah Code Ann. § 76-8-201.
- B. The SIAC reserves the right to restrict the qualifications and number of personnel having access to SIAC information and to suspend or withhold service to any personnel violating this privacy policy. The SIAC reserves the right to deny access to any participating agency user who fails to comply with the applicable restrictions and limitations of the SIAC's privacy policy.

XVI. Training

- A. The SIAC will require the following individuals to participate in training programs regarding the implementation of and adherence to this Privacy policy:
1. All SIAC employees and full-time contractors and consultants;
 2. All SIAC Intelligence Liaison Officers (ILOs), and participating analysts;
 3. Personnel providing information technology services or other services to the SIAC;
 4. Staff in other public or private agencies participating with the SIAC.
- B. The SIAC will provide special training to personnel authorized to share protected information through the Information Sharing Environment regarding the SIAC's requirements and policies for collection, use, and disclosure of protected information.

- C. The SIAC's Privacy Policy training programs will cover:
1. Purposes of the Information Privacy Policy;
 2. Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the SIAC;
 3. How to implement the policy in the day-to-day work of the user, whether a paper or systems user;
 4. The impact of improper activities associated with infractions within or through the SIAC;
 5. Mechanisms for reporting violations of the SIAC's Privacy Policy; and
 6. The nature and possible penalties for policy violations, including possible transfer, dismissal, civil and criminal liability, and immunity, if any.
- D. All reasonable efforts will be made to coordinate training efforts among all SIAC participants, where appropriate, to maximize the opportunity for training.

Appendix A: Glossary of Terms and Definitions

Access

In respect to privacy, an individual's ability to view, modify, and contest the accuracy and completeness of personally identifiable information collected about him or her. Access is an element of the Organization for Economic Co-operation and Development's (OECD) Fair Information Principles (FIPs). See *Fair Information Principles (FIPs)*.

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.

Accountability Principle

One of the eight Fair Information Principles (FIPs) developed by the Organisation for Economic Cooperation and Development (OECD). According to this principle, a data controller should be accountable for complying with measures that give effect to the principles stated above.

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.

Audit Trail

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

Authentication

Authentication is the process of validating the credentials of a person, computer process, or device. Authentication requires that the person, process, or device making the request provide a credential that proves it is what or who it says it is.

Common forms of credentials are digital certificates, digital signatures, smart cards, biometrics data, and a combination of user names and passwords. See Biometrics.

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

“Center” refers to the Statewide Information & Analysis Center and all participating state agencies of the Statewide Information & Analysis Center.

Civil Rights

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

Civil Liberties

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

Confidentiality

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

Credentials

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

Criminal Intelligence Information or Data

Information deemed relevant to the identification of and the criminal activity engaged in by an individual who or organization that is reasonably suspected of involvement in criminal acts. The record is maintained in a criminal intelligence

system per 28 CFR Part 23. Reasonable suspicion/criminal predicate applies to the information. The record is maintained per 28 CFR Part 23.

Criminal Intelligence System

The arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information [28 CFR Part 23.3 b (1)].

Criminal Predicate

See *Reasonable Suspicion*.

Data

Inert symbols, signs, descriptions, or measures.

Data Protection

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

Data Quality Principle

One of the eight Fair Information Principles (FIPs) developed by the Organisation for Economic Cooperation and Development (OECD). According to this principle, personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete, and up to date.

Data Transfer

As a key principle of privacy, it is the movement of personally identifiable information between entities, such as a customer list being shared between two different companies.

Disclosure

The release, transfer, provision of access to, or divulging of personally identifiable information in any other manner—electronic, verbal, or in writing—to an individual, agency, or organization outside of the agency who collected it.

Electronically Maintained

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

Electronically Transmitted

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

Enforcement

A privacy principle that provides mechanisms for ensuring compliance with the Organisation for Economic Co-operation and Development's (OECD) Fair Information Principles (FIPs), recourse for individuals affected by noncompliance, and consequences for noncompliant organizations. Methods for enforcement include a review by independent third parties.

Fair Information Principles (FIPs)

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

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 Participation Principle

One of the eight Fair Information Principles (FIPs) developed by the Organisation for Economic Co-operation and Development (OECD). As stated in

the FIPs, according to this principle, an individual should have the right:

- A. To obtain from the data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
- B. To have communicated to him, data relating to him:
 - 1. Within a reasonable time;
 - 2. At a charge, if any, that is not excessive;
 - 3. In a reasonable manner; and
 - 4. In a form that is readily intelligible to him;
- C. To be given reasons if a request made under subparagraphs a) and b) is denied, and to be able to challenge such denial; and
- D. To challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed, or amended.

Information

The use of data to extract meaning. Information includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists. Information received by law enforcement agencies can be categorized into three general areas: general data, tips and leads data, and criminal intelligence data.

Furthermore, information is data that may include records, documents, or files pertaining to law enforcement operations, such as computer-aided dispatch (CAD) data, incident data, and management information; data 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.

Information Disclosure

The exposure of information to individuals who normally would not have access to it.

Information Privacy

Information privacy is the interest individuals have in controlling or at least significantly influencing the handling of data about themselves.

Information Quality

The accuracy and validity of the actual values of the data, data structure, and database/data repository design. The elements of information quality are accuracy, completeness, currency, reliability, and context/meaning.

Information Sharing Environment (ISE)

In accordance with Section 1016 of the Intelligence Reform and Terrorism Prevention Act (IRTPA), as amended, the ISE will be composed of policies, procedures, and technologies linking the resources (people, systems, databases, and information) of state, local, and tribal (SLT) and federal entities and the private

sector to facilitate terrorism information sharing, access, and collaboration. Consistent with Presidential Guideline 5, the U.S. Attorney General, the U.S. Department of Justice (DOJ), and the Director of National Intelligence (DNI)—in coordination with the Program Manager for the ISE (PM-ISE) and the heads of federal departments and agencies that possess or use intelligence or other terrorism-related information—developed privacy guidelines for the ISE, titled Guidelines to Ensure That the Information Privacy and Other Legal Rights of Americans Are Protected in the Development and Use of the Information Sharing Environment (ISE Privacy Guidelines). The ISE Privacy Guidelines describe the means by which federal departments and agencies participating in the ISE will protect privacy and civil liberties in the development and operation of the ISE.

According to the ISE Privacy Guidelines, “Protected information should be shared through the ISE only if it is terrorism information, homeland security information, or law enforcement information related to terrorism (terrorism-related information).” Fusion centers are anticipated to serve as the primary points of contact within states or regions for further dissemination of terrorism-related information consistent with DOJ’s Fusion Center Guidelines and applicable SLT laws and regulations. As the ISE develops, fusion centers and possibly other SLT agencies receiving information or sharing terrorism-related information will be required to parallel the ISE Privacy Guidelines in their privacy policies to be eligible to access and use federal agency ISE information. The ISE Privacy Guidelines state “that such nonfederal entities develop and implement appropriate policies and procedures that provide protections that are at least as comprehensive as those contained in these Guidelines.” In preparation for this requirement, this privacy policy has incorporated the primary components of the ISE Privacy Guidelines.

Intelligence System

See *Criminal Intelligence System*.

Invasion of Privacy

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

Investigation

As used by this policy, in addition to its traditional meaning, investigation includes the necessary research and analysis of law enforcement and threat information to determine reasonable suspicion and the likelihood of potential criminal activity. Investigation also includes the research and analysis techniques used to assist open investigations when reasonable suspicion has already been established.

Law

As used by this policy, law includes any local, state, or federal statute, ordinance, regulation, executive order, policy, or court rule, decision, or order as construed by appropriate local, state, or federal officials or agencies.

Law Enforcement Information

For purposes of the 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.

Logs

Logs are a necessary part of an adequate security system, as they are needed to ensure that data is properly tracked and only authorized individuals are getting access to the data.

Maintenance of Information

The 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 content. An item of metadata may describe an individual content item or a collection of content items. Metadata is used to facilitate the understanding, use, and management of information. The metadata required for this will vary based upon the type of information and context of use.

Openness Principle

One of the eight Fair Information Principles (FIPs) developed by the Organisation for Economic Co-operation and Development (OECD). According to this principle, there should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data and the main purposes of their use, as well as the identity and usual residence of the data controller.

Personal data

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

Personal Information

See *Personally Identifiable Information*.

Personally Identifiable Information

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

- A. 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).
- B. A unique set of numbers or characters assigned to a specific individual (including name, address, phone number, social security number, e-mail address, driver's license number, financial account or credit card number and associated PIN number, Automated Integrated Fingerprint Identification System [AIFIS] identifier, or booking or detention system number).
- C. Descriptions of event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records).
- D. 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

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

Privacy Policy

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

Privacy Protection

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

Protected Critical Infrastructure Information (PCII) Program

The Protected Critical Infrastructure Information (PCII) Program, established pursuant to the Critical Infrastructure Information Act of 2002 (CII Act), creates a framework which enables members of the private sector to voluntarily submit confidential information regarding the nation’s critical infrastructure to the Department of Homeland Security (DHS) with the assurance that the information, if it satisfies the requirements of the CII Act, will be protected from public disclosure. The PCII Program seeks to facilitate greater sharing of critical infrastructure information among the owners and operators of the critical infrastructures and government entities with infrastructure protection responsibilities, thereby reducing the nation’s vulnerability to terrorism.

Protected Information

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

Public

A. Public includes:

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

4. 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.
- B. Public does not include:
1. Employees of the agency;
 2. People or entities, private or governmental, who assist the agency in the operation of the justice information system, and agency in the operation of the justice information system; and
 3. Public agencies whose authority to access information gathered and retained by the agency is specified in law.

Public Access

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

Purpose Specification Principle

One of the eight Fair Information Principles (FIPs) developed by the Organisation for Economic Co-operation and Development (OECD). According to this principle, the purposes for which personal data are collected should be specified no later than at the time of collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Reasonable Suspicion

"Reasonable suspicion" (or, criminal predicate) is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise." US Department of Justice, Code of Federal Regulations 28 Part 23.20(c).

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.

Retention

Keeping or holding of data, records, information, and/or intelligence. The act of retaining something or the condition of being retained.

Retrievable Information

Information is retrievable in the ordinary course of business if it can be retrieved by taking steps that are taken on a regular basis in the conduct of business with respect to that information or that an organization is capable of taking with the procedures it uses on a regular basis in the conduct of its business. Information is not considered retrievable in the ordinary course of business if retrieval would impose an unreasonable burden or violate the legitimate rights of a person that is

not the subject of the information. The unreasonableness of burden is balanced against the significance of the information's use.

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.

Secondary Data Uses

Uses of personally identifiable information for purposes other than those for which the information was originally collected. The Organisation for Economic Co-operation and Development's (OECD) Fair Information Principles (FIPs) state that a person can provide personally identifiable information for a specific purpose without the fear that it may later be used for an unrelated purpose without that person's knowledge or consent.

Security

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

Security Policy

A security policy is different from a privacy policy. A security policy alone may not adequately address the protection of personally identifiable information or the requirements of a privacy policy in their entirety. A security policy addresses information classification, protection, and periodic review to ensure that information is being stewarded in accordance with an organization's privacy policy. See *Privacy Policy*.

Security Safeguards Principle

One of the eight Fair Information Principles (FIPs) developed by the Organisation for Economic Co-operation and Development (OECD). According to this principle, personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data.

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:

- A. Storage is frequently used to mean the devices and data connected to the computer through input/output operations—that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-computer storage. This meaning is probably more common in the IT industry than meaning B.
- B. In a more formal usage, storage has been divided into (1) primary storage, which holds data in memory (sometimes called random access memory or RAM) and other “built-in” devices such as the processor’s L1 cache, and (2) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations.

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

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

Suspicious Activity

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

Suspicious Activity Report (SAR) Information

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 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 IRTPA, as recently amended by the 9/11 Commission Act enacted on August 3, 2007 (P.L. 110-53), the ISE facilitates the sharing of terrorism and homeland security information, as defined in IRTPA Section 1016(a)(5) and the Homeland Security Act 892(f)(1) (6 U.S.C. § 482(f)(1)). See also Information Sharing Environment Implementation Plan (November 2006) and Presidential Guidelines 2 and 3 (the ISE will facilitate the sharing of “terrorism information,” as defined in IRTPA, as well as the following categories of information to the extent that they do not otherwise constitute “terrorism information”: (1) homeland security information as defined in Section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. § 482(f)(1)); and (2) law enforcement information relating to terrorism or the security of our homeland). Such additional information includes intelligence information.

Weapons of Mass Destruction (WMD) information as a fourth (third statutory) category of ISE information is not called for in P.L. 110-53. Rather, it amends the definition of terrorism information to include WMD information and then defines that term. WMD information probably should not technically be cited or referenced as a fourth category of information in the ISE.

Tips and Leads Information or Data

Uncorroborated report or information generated from inside or outside the agency that alleges or indicates some form of possible criminal activity. Tips and leads can also be referred to as suspicious incident report (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 is maintained in a secure system, similar to data that rises to the level of reasonable suspicion.

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

Transborder Flows of Personal Data

Movements of personal data across national borders. See *Fair Information Principles (FIPs)*.

Use

With respect to personally identifiable information, the sharing, employment, application, utilization, examination, or analysis of such information within the agency or organization that maintains the designated record set.

Use Limitation Principle

One of the eight Fair Information Principles (FIPs) developed by the Organisation for Economic Co-operation and Development (OECD). According to this principle, personal data should not be disclosed, made available, or otherwise be used for purposes other than those specified in accordance with the Purpose Specification Principle, except with the consent of the data subject or by the authority of law. See *Purpose Specification Principle*.