Utah Statewide Information & Analysis Center

Information Privacy Policy

Mission

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.

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 any 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.

Statutory Authority

The Utah Department of Public Safety is granted statutory authority under Utah Code Ann. §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)] as defined in 28 CFR Part 23.3 b (1).
G. Provide specialized case support and investigate illegal drug production, cultivation, and sales [53-10-302 (8)].
H. Investigate, follow-up, and assist in highway drug interdiction cases [53-10- 302 (9)].

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 and applicable laws protecting privacy, civil rights, and civil liberties.

This Privacy Policy provides authoritative guidance and direction, and establishes the policies and procedures regarding the manner in which information is collected, received, maintained, stored, accessed, disclosed, or disseminated to SIAC personnel, governmental agencies ,private contractors, private entities, and the general public.

All other 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 not be governed by this policy, but will be handled in a manner which complies with all applicable privacy laws, regulations, and internal policies.

All SIAC users including assigned or detailed personnel, information technology service providers, private contractors, and other authorized participants in any SIAC operational component shall be provided with a copy and comply with this Privacy Policy and all applicable laws protecting privacy, civil rights, and civil liberties.

Governance and Oversight

The Utah Department of Public Safety has the primary responsibility for the operation of the SIAC.

A Governance Board, established by the Utah Department of Public Safety:

A. provides oversight of SIAC operations,
B. is responsible for the review and approval of all SIAC policies including the Privacy Policy,

C. is responsible for ensuring audits of all SIAC records for compliance with the Privacy Policy and applicable laws, and
D. may recommend the suspension of a participant agency for due cause and recommend, if appropriate, the reinstatement of a suspended participant agency.

The SIAC Bureau Chief will designate a trained Privacy Officer who is responsible for handling reported errors and violations. The Privacy Officer will be the focal point for ensuring that the SIAC adheres to the Privacy Policy. The SIAC Bureau Chief, with the assistance of the SIAC Privacy Officer, shall retain responsibility for ensuring that the Privacy Policy is rigorously implemented reviewed, and updated annually.

The designated Privacy Officer can be contacted at SIAC@utah.gov or 801.256.2360.

Retention of Information

The primary sources of information to the SIAC are other governmental entities, including other Utah law enforcement agencies and SIAC Intelligence Liaison Officers, various information systems operated by governmental entities, and searches of publicly available records including those accessible through the Internet.

The SIAC will only seek, collect, or retain information that was collected in a fair and lawful manner and is:

A. Based on reasonable suspicion that an individual or organization has committed or is involved in, supporting, facilitating or planning a criminal offense or criminal (including terrorist) conduct.
B. Relevant to the assessment of criminal information; 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.
C. Useful in a crime or threat analysis or otherwise in furtherance of the public safety or homeland security responsibilities of the SIAC; provided that the source of the information is reliable or limitations on the quality of the information have been identified.

The SIAC will not directly or indirectly seek, retain, or accept 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:

A. Relevant to whether an individual or organization has engaged in, is engaging in, or is planning criminal (including terrorist) activity.
B. Relevant to ongoing law enforcement investigations or emergency situations.

C. Needed by the SIAC or partner agencies to identify an individual or to provide services to the individual or accommodate an individual's religious, ethnic, or cultural requests or obligations.

Classification of Information Regarding Validity and Reliability

SIAC personnel will, upon receipt of information, assess the information to determine its nature, usability, and quality. As appropriate, personnel will classify the information (or ensure that the originating agency has classified the information) as outlined in the SIAC Standard Operating Procedures.

Such classification 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.

The classification of existing information will be re-evaluated and updated when new information is gathered that has an impact on the validity and reliability of retained information.

Tips, Leads and Suspicious Activities Reports

The SIAC routinely receives tips, leads, and suspicious activity reports (SAR). SIAC personnel evaluate and assess the information and, where appropriate, forward it to partner agencies in accordance with applicable SIAC policies and procedures for a valid public safety or law enforcement purpose. The SIAC adheres to national standards for the suspicious activity reporting process, including the use of a standard reporting format and commonly accepted data collection codes and a sharing process that complies with the Information Sharing Environment (ISE) Functional Standard for suspicious activity reporting.

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, leads and SAR information. SIAC personnel will:

A. prior to allowing access to or dissemination of the information, ensure that attempts to validate or refute the information have taken place and that the information has been assessed for sensitivity and confidence by subjecting it to an evaluation or screening process to determine its credibility and value, and categorize the information as unsubstantiated or uncorroborated if attempts to validate or determine the reliability of the information have been unsuccessful;
B. 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;
C. 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);

D. regularly provide access to or disseminate the information in response to an interagency inquiry for law enforcement, homeland security, or public safety and analytical purposes, or provide an assessment of the information to any agency, entity, individual, or the public when credible information indicates potential imminent danger to life or property.

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 or terrorism activities will be documented and shared through the ISE, eGuardian, and the SAR Data Repository. These safeguards are intended to ensure that information that could violate civil rights and civil liberties will not be intentionally or inadvertently gathered, documented, processed, and shared.

SAR information submitted into an external SAR repository, such as ISE, eGuardian, or SAR Data Repository 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.

Information Quality Assurance

The SIAC will make every reasonable effort to ensure that information sought or retained is:

A. derived from dependable and trustworthy sources of information,
B. accurate,
C. current/relevant,
D. complete, and
E. merged with other information about the same individual or organization only when the applicable standard has been met.

Such standards must be met when records are used to make any determination about an individual. 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.

SIAC personnel will appropriately review all information to ensure its suitability and approve or deny its retention prior to the information being retained within any SIAC system.

The classifying 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.

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:

A. the name of the originating department, component, and subcomponent;
B. the date the information was collected, and where feasible, the date its accuracy was last verified;
C. the title and contact information for the person to who questions regarding the information should be directed; and
D. articulation of an authorized law enforcement purpose for collecting and retaining the information.

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.

The SIAC shall keep a record of all sources of information retained. 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.

Acquiring and Receiving Information

The SIAC will comply with applicable accepted information gathering (acquisition and access) and investigative techniques as outlined in 28 CFR Part 23 regarding criminal intelligence information, and require similar compliance from information-originating agencies.

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.

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.

The SIAC will not directly or indirectly receive, seek, accept, or retain information from 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.

Information acquired, received or accessed by the SIAC from other sources will only be analyzed:

A. 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. to further crime (including terrorism) prevention, enforcement, force deployment, or prosecution objectives and priorities established by the SIAC and partner agencies;
C. to 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;
D. to 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).

Merging of Information from Different Sources

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 individual or organization may include the name, federal or state tax ID number, office address, and telephone number.

Information Sharing, Dissemination, and Disclosure

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.

The SIAC will comply with court orders for dissemination issued in compliance with Utah Code Ann. § 63G-2-207. Records of all such orders and information disclosed shall be kept.

Sharing Information with Those Responsible for Public Protection, Safety, or Public Health

Information 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.

Criminal intelligence information may be disseminated to law enforcement, homeland security, or counterterrorism agencies for any type of 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.

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.

Sharing Information for Specific Purposes

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 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.

Disclosing Information to the Public

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 the Utah Government Records Access Management Act (GRAMA) or applicable provisions of law. Such information may be disclosed only in accordance with the law and procedures applicable to the SIAC for this type of information.

An audit trail will be kept of all requests and of what information is disclosed to a member of the public.

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

A. Criminal investigative information and criminal intelligence information. These records are classified as protected under Utah Code Ann. § 63G-2- 305.
B. Information containing data on individuals the disclosure of which constitutes a clearly unwarranted invasion of personal privacy under Utah Code Ann. § 63G-2-302 or other applicable federal law or regulation.
C. 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.

D. 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) under the Critical Infrastructure Information Act of 2002.
E. Other records and information as set forth by federal and state law.

A record or part of a record that has 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.

Privacy Safeguards

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.

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.

Information gathered and records retained by the SIAC will not be:

A. sold, published, exchanged, or disclosed for commercial purposes;
B. disclosed or published without prior notice to the contributing agency that such information is subject to re-disclosure or publication;
C. disseminated to unauthorized persons.

The SIAC will include an appropriate handling notice on all transmitted documents when information is disseminated.

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.

Disclosing Information to the Individual about Whom Information has Been Gathered

Upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity and subject to the conditions specified 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.

If an individual requests information about him or her that originates with another agency, the SIAC Privacy Officer will refer the individual to the source agency.

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:

A. Disclosure would interfere with ongoing investigations [Utah Code Ann. § 63G-2-305].
B. Disclosure would endanger the life or safety of an individual [Utah Code Ann. §63G-2-305].
C. The information is in a criminal intelligence system subject to 28 CFR Part 23 [28 CFR 23.20(e)].
D. The information concerns security measures designed for the protection of persons or property, public or private [Utah Code Ann. § 63G-2-106].
E. The information could reasonably be expected to reveal the identity of a source not generally known outside of government [Utah Code Ann. § 63G-2-305].
F. The information could reasonably be expected to reveal investigative techniques, procedures, policies, or orders not generally known outside of government [Utah Code Ann. § 63G-2-305].
G. Other authorized basis for denial exists.

Complaints and Corrections

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 Officer will inform the individual of the procedure for submitting complaints or requesting corrections, by mail, e- mail, or in person. 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 working days of receipt of the complaint or request.

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.

Upon receipt of a complaint or request for correction, the SIAC Privacy Officer will consent to the correction, remove the record, or state in writing a basis for the denial of the complaint or request. All denials will be reviewed and approved by the SIAC Bureau Chief.

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 Officer will notify the source agency of the complaint or correction request and use reasonable efforts to 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.

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 ISE, eGuardian or the SAR Data Repository 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 Privacy Officer 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. Any personal information originating with the SIAC will be reviewed within 30 days and confirmed, corrected or deleted from SIAC data/records if it is determined to be erroneous, include incorrectly merged information, or is 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.

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 Commissioner of the Department of Public Safety.

Security Safeguards

A SIAC employee will be designated and trained to serve as the SIAC Security Officer.

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.

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 under 28 CFR Part 23.

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.

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.

Whenever possible, queries made to SIAC data applications will be automatically logged into each respective data system identifying the user, date, and time of the query.

The SIAC will utilize record logs to maintain records of requested, sought, collected, and disseminated information.

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

Violations of this policy or internal operating policies at the SIAC will be reported to the SIAC Bureau Chief or his or her designee.

Destruction of Information

All information stored in the SIAC database other than analytical product will be reviewed for record retention (validation or purged) at least every five (5) years. 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.

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.

The SIAC will delete information or return it to the source, unless it is validated as specified in 28 CFR Part 23.

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:

A. The information is erroneous, misleading, obsolete, or otherwise unreliable.
B. The source of the information did not have authority to gather the information or to provide the information to the SIAC.
C. 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.

Accountability and Enforcement Regarding Information System Transparency

This Information Privacy Policy will be made available to the public on request and through any public web sites providing information about the SIAC.

The SIAC's Privacy Officer 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

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 resides with the SIAC Bureau Chief or his designee.

The SIAC will strive to protect information from unauthorized access, modification, theft, or sabotage, whether internal or external and whether due to natural or human-caused disasters or intrusions.

The SIAC will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with the use of data systems, 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 SIAC.

The SIAC will maintain an audit trail of accessed, requested, or disseminated information. An audit trail will be kept for 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.

The SIAC will require any individuals authorized to use the system to agree 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 signed agreement to comply with this policy and the provisions it contains.

At the direction of the SIAC Governance Board, independent, non-SIAC personnel will conduct audits and inspections of the information contained in SIAC's record management system at least once per year. All audits will be conducted in a manner that protects the confidentiality, sensitivity, and privacy of all stored information.

SIAC management may order periodic, internal audits of its information systems to ensure compliance with this privacy policy.

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.

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 Officer and/or the SIAC Bureau Chief.

Inadvertent Disclosure

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. The SIAC shall investigate the scope of the release of information and, if necessary, reasonably restore the integrity of any information system affected by this release.

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.

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.

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.

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:

A. Social security number.
B. Driver's license number or Utah Identification Card number.
C. 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.
D. Medical information.
E. Health insurance information.

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.

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.

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.

For purposes of this section, "notice" may be provided by one of the following methods:

A. Written notice.
B. Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set in Section 7001 of Title 15 of the U.S. Code.
C. 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 an e-mail notice when the SIAC has an e-mail address for the subject person(s) or other reasonable means of providing notice.

Enforcement

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. This includes the following:

A. Suspend or discontinue access to information by the user.
B. Counsel, reprimand, suspend, demote, transfer, or terminate the person as permitted by applicable personnel policies.
C. Apply other sanctions or administrative actions as provided by DPS rules and regulations or as provided in SIAC personnel policies.
D. 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.
E. Refer the matter to appropriate authorities for criminal prosecution, if appropriate.

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.

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.

Training

All reasonable efforts will be made to coordinate training efforts among all SIAC participants, where appropriate, to maximize the opportunity for training.

The SIAC will require the following individuals to participate in training programs regarding the implementation of and adherence to this Privacy policy:

A. all SIAC employees and full-time contractors and consultants,
B. all SIAC Intelligence Liaison Officers (ILOs), and participating analysts, and
C. personnel providing information technology services or other services to the SIAC.

The SIAC will provide training to personnel authorized to share protected information through the ISE, SAR Data Repository, or eGuardian regarding the SIAC's requirements and policies for collection, use, and disclosure of protected information.

The SIAC's Privacy Policy training programs will cover:

A. purposes of the Information Privacy Policy;
B. 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;
C. how to implement the policy in the day-to-day work of the user, whether a paper or systems user;
D. the impact of improper activities associated with infractions within or through the SIAC;
E. mechanisms for reporting violations of the SIAC's Privacy Policy; and
F. the nature and possible penalties for policy violations, including possible transfer, dismissal, civil and criminal liability, and immunity, if any.

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 SAR Data Repository (SDR), 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 SDR participant

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 SDR 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 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.

Biometrics

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

Civil Rights

The term “civil rights” is used to imply that the state has a role in ensuring 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 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)].

Data

Includes, documents, inert symbols, signs, descriptions, or measures.

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.

Homeland Security Information

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

Identification

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

Information

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 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.

Intelligence System

See *Criminal Intelligence System*.

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 this policy, 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.

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.

Operational Components

These include Intelligence Analysis, Intelligence Liaison Officer Program, and Critical Infrastructure Protection.

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.

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 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.

With regards to state government, protected information is defined in the Utah Government Records Access and Management Act. See Utah State Code 63G-2-305. While a detailed explanation can be found in the statute, protected information essentially refers to records that contain information that, if released could have an adverse effect on government operations that would outweigh the societal benefits of disclosure.

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.

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.

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.

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*.

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

Suspicious Activity

Defined in the ISE-SAR Functional Standard 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.

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.