California
State Terrorism Threat Assessment System
Information Privacy Policy

Mission:

The California State Terrorism Threat Assessment System (STTAS) is a collaborative effort to lawfully and appropriately gather and analyze information, employ analytical tools and methodologies to produce and share timely and actionable homeland security information between agencies and across the full range of public safety disciplines. The STTAS consists of four Regional Terrorism Threat Assessment Centers (RTTACs) and a single state-wide center: the Northern California Regional Intelligence Center; the Los Angeles Joint Regional Intelligence Center; the San Diego Law Enforcement Coordination Center; the Central California Intelligence Center; and, California State Terrorism Threat Assessment Center (STTAC).(Hereinafter collectively referred to as "STTAS Components".)

Policy Applicability and Legal Compliance

The STTAS Information Privacy Policy ("Privacy Policy") provides authoritative guidance, direction and establishes the policies and procedures regarding the manner in which information is collected, received, maintained, archived, accessed, or disclosed within the STTAS, and disclosed to other governmental entities, private contractors, and the general public.

The Privacy Policy applies to information about individuals and organizations obtained by the STTAS in furtherance of its analytical mission. 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 STTAS as governmental entities) 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.

The STTAS, and all assigned or detailed personnel, shall comply with all laws and regulations that govern the handling of national security classified information. This policy does not apply to national security classified information.

The STTAS, and all assigned or detailed personnel, including personnel providing information technology services, private contractors, and other authorized participants in any STTAS Component, shall 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 internal operating policies of each STTAS Component will be consistent with this Privacy Policy and will incorporate applicable laws protecting privacy, civil rights, and civil liberties. The desired outcome of this policy is to protect the privacy rights of US persons.

Retaining Information

What Information May Be Retained?

STTAS Components will not retain information that was not collected in a lawful manner. STTAS Components will comply with 28 C.F.R. Part 23, the California Attorney General's Model Standards and

Procedures for Maintaining Criminal Intelligence Files (CA AG's Guidelines) and the California Constitution and, with regard to the State Terrorism Threat Assessment Center (STTAC), the California Information Practices Act (Gov. Code § 1798 et seq.).

All STTAS Components may only place information in criminal intelligence files and/or retain information:

1. Where there is reasonable suspicion that a specific 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, California, or the nation and the information is relevant to the criminal (including terrorist) conduct or activity; or,

2. 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, California, or the nation and the information is relevant to the criminal (including terrorist) conduct or activity.

3. That is relevant to the identification of a criminal suspect or to the criminal activity in which the suspect is engaged may be filed and retained provided that (1) the information is labeled as "Non-Criminal Identifying Information"; (2) identifying information may not be used as an independent basis to meet the requirement of reasonable suspicion of involvement in criminal (including terrorist) activity; and, (3) the individual or organization which is the criminal suspect identified by this information otherwise meets all requirements of 28CFR Part 23. We are mindful of the recommendation within the CA AG's Guidelines that such information not be included in criminal intelligence files. 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.

4. That is useful in a crime or threat analysis or otherwise in furtherance of the public safety, anti-terrorism, counter-terrorism, or homeland security responsibilities of the STTAS and its components; provided that the source of the information is reliable or limitations on the quality of the information have been identified.

5. Such as tips, leads, or suspicious activity reports, which is based on mere suspicion of criminal (including terrorist) activity that falls within the public safety, anti-terrorism, counter-terrorism, or homeland security responsibilities of the STTAS and each component fusion center.

Information that shall be specifically excluded from criminal intelligence files includes:

a. Information on an individual or group merely on the basis that such individual or group supports unpopular causes.
b. Information on an individual or group merely on the basis of race, gender, age, or ethnic background.
c. Information on an individual or group merely on the basis of religious or political affiliations or beliefs.

d. Information on an individual or group merely on the basis of personal habits and/or predilections that do not violate any criminal laws or threaten the safety of others.
e. Information on an individual or group merely on the basis of involvement in expressive activity that takes the form of non-violent civil disobedience that amounts, at most, to a misdemeanor offense.

Methods of Seeking or Receiving Information

(a) The primary sources of information to each STTAS Component are other governmental entities, including the member organizations that comprise each Component (through various information systems operated by governmental entities, and through searches of publicly available records, particularly those accessible through the Internet). Information gathering techniques used by this agency will comply with all applicable laws.

(b) STTAS Components will not directly or indirectly receive, seek, accept, or retain information from an individual or nongovernment information provider if the agency 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 agency.

(c) STTAS Components will maintain a record of information sought and received.

(d) While the member organizations of each STTAS Component may have criminal investigative authorities and responsibilities, the STTAS Components, when acting as a fusion center, do not conduct investigations.

Classification of Information Regarding Validity and Reliability

(a) At the time of retention, the information will be categorized regarding it's:

1. Content validity;
2. Nature of the source;
3. Source reliability;
4. Accuracy;
5. Completeness; and,
6. Currency

(b) At the time a decision is made to retain information, it will be classified pursuant to the applicable limitations on access and sensitivity of disclosure in order to:

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 and civil rights;
4. Provide legally required protection based on the status of an individual as a victim or witness,

(c) STTAS Component personnel will assess the information to determine its nature and purpose. Personnel will assign information to categories to indicate the result of the assessment, such as:

1. Whether the information is general data, tips and leads data, suspicious activity reports, or criminal intelligence information;
2. The nature of the source (for example, anonymous tip, interview, public records, private sector);
3. The reliability of the source (i.e., reliable, usually reliable, unreliable, unknown); and
4. The validity of the content (i.e., confirmed, probable, doubtful, cannot be judged).

(d) 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.

(e) STTAS Components shall keep a record of the source of information retained by that Component. In this context, "source" refers to the individual or entity which provided the information to the Component. 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, a long as the specific unit of that agency, governmental entity, or organization which provided the information is identified.

(f) These 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) STTAS Components will make reasonable efforts, including the use of appropriate contractual requirements, to ensure that information obtained from commercial databases was collected using lawful techniques

(h) Information which pertains to U.S. Persons or is subject to specific restrictions on access, use or disclosure will be marked appropriately.

Temporary Files

Information may be entered into temporary files when a determination has been made that, although the reasonable suspicion standard for an individual and/or organization has not been met, there is a reasonable likelihood that wthin one year the standard for entry into the criminal intelligence file system may be available. Temporary files shall not be retained for longer than one-year. At the end of one year, temporary files must either be purged or converted into criminal intelligence files, if the information satisfies the criteria for submission into criminal intelligence files. A temporary file is considered purged for this purpose if all of the personally identifiable information (or privacy field data) is removed, deleted, and destroyed. All temporary files shall be specifically designated as such and they will be kept distinctly separate from criminal intelligence files.

The most common categories of temporary files are SUSPICIOUS Activity Reports (SARs) and Tips and Leads.

Tips, Leads, and Suspicious Activity Reports

STTAS Components routinely receive tips, leads, or other reports of suspicious activities. Component personnel evaluate the information and, where appropriate, forward it to the Regional Terrorism Threat Assessment Advisory Center (RTTAC) or RTTACs with geographic responsibility for further evaluation or investigation of the tip, lead or report in accordance with applicable procedures and direction provided by the RTTAC leadership. Depending on the nature of the information, and particularly when credible information indicates a potential danger to life and property, the Component may report the information to CHP, Cal EMA and other governmental entities with law enforcement, counterterrorism, or national security responsibilities. The STTAC does not conduct investigative activity based on tips, leads or suspicious activity reports.

With regard to tips, leads, or suspicious activity reports, STTAS Component personnel will:

1. 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;
2. 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;
3. Adhere to and follow the Component's physical, administrative, and technical security measures that are in place for the protection and security of tips and leads information. Tips, leads, and SARs 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.

STTAS Components will seek or retain information that a source agency has determined constitutes "suspicious activity" and which:

1. Is based on (a) a criminal predicate or (b) a possible threat to public safety; including potential terrorism-related conduct; and
2. Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; or the prevention or crime; and
3. The source agency assures was acquired in accordance with agency policy and in a lawful manner.

STTAS Components will not retain suspicious activity report information about any individual that was gathered solely on the basis of that individual's religious, political, or social views or activities; participation in a particular noncriminal organization or lawful event; or race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation.

Upon receipt of SAR information from a source agency, STTAS Component personnel will:

Personally review and vet the SAR information and make the appropriate assessment in accordance with guidelines governing the system within which the information is stored (such as ISE-SAR, e-Guardian, COPLINK etc.)

Ensure that any information posted to a SAR repository includes appropriate labels;
Notify the source agency of the disposition of the SAR information.

The STTAS component will ensure that certain basic and special descriptive information is entered and electronically associated with SAR information including:

1. The name of the source agency;
2. The date the information was submitted;
3. The point of contact information for SAR-related data; and
4. Information that reflects any special laws, rules or policies regarding access, use and disclosure.

Information provided in a SAR repository shall indicate, the maximum extent feasible:

1. The nature of the source: anonymous tip, confidential source; trained interviewer or investigator; written statement (victim, witness, other), private sector, or other source; and
2. Confidence, including:
    - The reliability of the source (reliable, unreliable or unknown); and
    - The validity of the content (confirmed, doubtful, or cannot be judged).
3. Due diligence will be exercised in determining source reliability and content validity. Information determined to be unfounded will be purged from the shared space.
4. 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.

At the time a decision is made to post SAR information to an external SAR repository such as ISE-SAR, e-Guardian, or COPLINK, STTAS Component personnel will ensure that the information is labeled to the maximum extent feasible and consistent with applicable standards, to reflect any limitations on disclosure based on sensitivity of disclosure, in order to:

1. Protect an individual's right of privacy, civil rights, and civil liberties;
2. Protect confidential sources and police undercover techniques and methods;
3. Not interfere with or compromise pending criminal investigations; and
4. Provide any legally required protection based on an individual's status 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.

STTAS Components 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. If subsequent attempts to validate the information confirm its validity or are unsuccessful, the information in the shared space will be updated (replaced) to so indicate. Information determined to be unfounded will be purged from the shared space.

STTAS Components will incorporate the gathering, processing, reporting, analyzing, and sharing of SAR information 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 the privacy, civil rights, and civil liberties of individuals.

Notice will be provided through data field labels or narrative information to enable authorized users to determine the nature of the protected information in the shared space and how to handle the information in accordance with applicable legal requirements, including any restrictions based on information security or classification.

Law enforcement officers and other personnel at source agencies who acquire SAR information that may be shared with the STTAS or a STTAS Component will be trained to recognize behavior that is indicative of criminal activity related to terrorism.

When a choice of investigative techniques is available, information documented as a SAR should be acquired or investigated using the least intrusive feasible means, taking into account such factors as the effect on individuals' privacy and potential damage to reputation.

Information Quality

A substantial portion of the information received by STTAS Components is in the form of completed analytical product. The STTAC does not use these products to conduct investigations or to support prosecutions but rather in furtherance of its mission to analyze and assess strategic threats to the state. The rigorous examination of information quality is a critical component of effective analysis. The member organizations of each RTTAC may use the information in furtherance of investigative or other activities within their jurisdiction and authority. However, STTAS Components are not responsible for providing feedback to other agencies regarding the analytical efforts or products of those agencies simply because the Component may not concur with the analysis. While some feedback may occur, it need not be formal or routine.

(a) STTAS Components 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;
4. Complete, including the relevant context in which it was sought or received and other related information; and
5. Merged with other information about the same individual or organization only when the applicable standard has been met.

(b) STTAS Components will make every reasonable effort to ensure that only authorized users are allowed to add, change, or delete information in the system.

(c) STTAS Components will actively research suspected errors and deficiencies and will make every reasonable effort to ensure that information will be deleted from the system when the agency learns that:

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 agency; or
3. The source of the information used prohibited means to gather the information.

(d) Originating agencies providing data remain the owners of the data contributed. STTAS Components will take reasonable steps to advise the appropriate data owner if its data is found to be inaccurate or incomplete where the Component is the primary or initial recipient of such information.

(e) STTAS Components shall maintain all records, to the maximum extent possible, with accuracy, relevance, timeliness, and completeness. Such standard need not be met except when such records are used to make any determination about the individual. When Component personnel transfer a record outside of the STTAS, the Component shall correct, update, withhold, or delete any portion of the record that it knows or has reason to believe is inaccurate or untimely. Each Component shall notify any recipient agency if information provided by the Component 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.

Collation and Analysis of Information

Collation and Analysis

(a) Information sought or received by the agency or from other sources will only be analyzed:

1. By qualified individuals who are authorized to access the information;
2. 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 generally; and
3. To further crime (including terrorism) prevention, enforcement, force deployment, or prosecution objectives and priorities established by the agency.
4. To create strategic, geographic region, or critical infrastructure sector, specific analysis products providing state, local and agency leadership with treat and risk assessment information upon which to base resource prioritization, information analysis and awareness decisions.

(b) Information sought or received by the agency or from other sources will not be analyzed or combined in a manner or for a purpose that violates this policy. Only information which has been properly collected and retained may be analyzed.

SAR Information posted to the shared space or accessed from the shared spaces will be analyzed for intelligence purposes only by qualified personnel who have successfully completed a background check and any applicable security clearance and have been selected, approved and trained accordingly (including training on the implementation of this policy). These personnel shall share SAR information only through authorized analytical products.

Merging of Information from Different Sources

(a) The set of identifying information sufficient to allow merging will utilize reasonable steps to identify the subject and may include the name (full or partial) and, in most cases, one or more of the following: date of birth; law enforcement or corrections system identification number; individual identifiers, such as fingerprints, photographs, physical description, height, weight, eye and hair color, race, ethnicity, tattoos, or scars; social security number; driver's license number; or other biometrics, such as DNA, retinal scan, or facial recognition. The identifiers or characteristics that, when combined, could clearly establish that the information from multiple records is about the same organization may include the name, federal or state tax ID number, office address, and telephone number.

(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 adequately established that the information relates to the same individual or organization.

Dissemination of Information

(a) STTAS Components will identify and review protected information that originated in the center prior to sharing that information in the ISE. Further, the center 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.

(b) In accordance with the Information Practices Act of 1977, the STTAC shall keep an accurate accounting of the date, nature, and purpose of each disclosure of a record made pursuant to subdivision (i), (k), (l), (o), or (p) of Civil Code Section 1798.24. This accounting shall also be required for disclosures made pursuant to subdivision (e) or (f) of Civil Code Section 1798.24 unless notice of the type of disclosure has been provided pursuant to Civil Code Sections 1798.9 and 1798.10. The accounting shall also include the name, title, and business address of the person or agency to which the disclosure was made. For the purpose of an accounting of a disclosure made under subdivision (o) of Civil Code Section 1798.24, it shall be sufficient for the STTAC to record the date of disclosure, the law enforcement or regulatory agency requesting the disclosure, and whether the purpose of the disclosure is for an investigation of unlawful activity under the jurisdiction of the requesting agency, or for licensing, certification, or regulatory purposes by that agency. Routine disclosures of information pertaining to crimes, offenders, and suspected offenders to law enforcement or regulatory agencies of federal, state, and local government shall be deemed to be disclosures pursuant to subdivision (e) of Civil Code Section 1798.24 for the purpose of meeting this requirement. STTAS Components other than the STTAC are not subject to the requirements of the Information Practices Act of 1977. The STTAC will assert all appropriate exemptions, including but not limited to Civil Code Section 1798.40.

The employees and users of the participating agencies and of the agency'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. STTAS Components will include a statement substantially similar to the following in the 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, receipt 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."

SAR information submitted into an external SAR repository such as ISE-SAR or e-Guardian and retained by a STTAS Component will be accessed by or disseminated only to persons within the STTAS 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 for legitimate law enforcement and public protection purposes and only for the performance of official duties in accordance with law.

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

(a) Information retained by Components may be disseminated to individuals in public or private entities only for public protection, safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures.

(b) 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 Component's compliance with 28 CFR Part 23. Participating agencies that access information from a STTAS Component must comply with any applicable dissemination limitations or practices imposed by the STTAS Component or the originator of the information. This may, or may not, include obtaining approval of the originator prior to further dissemination.

(c) 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.

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

Sharing Information for Specific Purposes

(a) Information gathered and retained by this agency may be disseminated for specific purposes upon request by persons authorized by law to have such access and only for those uses or purposes specified in the law.

(b) An audit trail will be kept of the requests for access and of what information is disseminated to such persons.

Disclosing Information to the Public

(a) Information gathered and retained by STTAS Components may be disclosed to a member of the public in accordance with the California Public Records Act, the Information Practices Act, or otherwise in a manner consistent with applicable law and the public interest.

(b) Information gathered and records retained by STTAS Components ***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 redisclosure or publication; or
3. Disseminated to unauthorized persons.

(c) 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 California Public Records Act or applicable provisions of federal laws, regulations, and executive orders, which govern the disclosure of classified or sensitive but unclassified information.

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

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

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

1. Public records required to be kept confidential by law are exempted from disclosure requirements under the Freedom of Information Act (FOIA), California Public Records Act (CPRA), Critical Infrastructure Information Act of 2002, among other provisions of law.
2. For instance, law enforcement records described in Gov Code §6254(f) will not be released to the public in accordance with the provisions of the CPRA.

(g) SAR information posted to the shared space or submitted to an external SAR repository may be disclosed to a member of the public only if the information is defined by law to be a public record or otherwise appropriate for release to further the STTAS or STTAS Component 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 STTAS Component for this type of information.

(h) 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 CPRA, including but not limited to sections 6254(f), (aa), (ab) and 6255. This includes a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism under or an act of agricultural terrorism, vulnerability assessments, risk planning documents, needs assessments, and threat assessments.

Disclosing Information to the Individual about Whom Information Has Been Gathered

(a) To the extent information is maintained in information systems controlled by the State of California, STTAS Components will comply with the Information Practices Act of 1977 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 STTAS Component 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 *within a system under the Component's control*, the Component will advise the individual of the process to submit a request for correction by mail or e-mail. 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. 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 10 working days of receipt of the complaint or request. 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. This process will be specific to each STTAS Component. The STTAS Component Commander or his or her designee will determine whether the complaint or request involves ISE or FBI information and will review and approve the response.

(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 Component will notify the originating agency of the complaint or correction request and coordinate with them to ensure that the individual is provided with complaint submission or correction procedures. When the complaint pertains to the correction of a record that has been disclosed to the complainant, the originating agency must either consent to the correction, remove the record, or assert a basis for denial in accordance with the California Public Records Act (CPRA) or Information Practices Act (IPA). This must be done in sufficient time to permit compliance with deadlines found within CPRA and/or IPA. A record will be kept of all complaints and correction requests

Review of Information Regarding Retention

(a) Information other than analytical product will be reviewed for purging every five years. Information may be reviewed through automated or other means consistent with resource constraints and availability. Records need not be individually examined to comply with this requirement. The date and means of review will be documented.

(b) When information has no further value or meets the criteria for removal under applicable law, it will be purged, destroyed, deleted, or returned to the submitting source.

Security Safeguards

(a) The Assistant Director for Information Analysis, Watch and Warning is designated and trained to serve as the STTAS security officer.

(b) STTAS Components will operate in a secure facility protecting the facility from external intrusion. Each component will utilize secure internal and external safeguards against network intrusions. Access to databases from outside the facility will only be allowed over secure networks.

(c) STTAS Components 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.

(d) Access to center information will only be granted to center personnel whose position and job duties require such access and the individual has successfully completed a background check and appropriate security clearance, if applicable, and has been selected, approved, and trained accordingly.

(e) Queries made to the component data applications will be logged into the data system identifying the user initiating the query.

(f) STTAS Components will maintain appropriate documentation to preserve audit trails of requested and disseminated information.

(g) Information will be marked appropriately if subject to specific handling caveats or other restrictions on storage, dissemination, use or destruction.

(h) To prevent 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 each STTAS Component will be reported to the STTAS Component Commander or his or her designee.

Information Retention and Destruction

1. All applicable information will be reviewed for record retention (validation or purge) at least every five (5) years, as provided by 28 CFR Part 23.

2. When information has no further value or meets the criteria for removal according to applicable law, it will be purged, destroyed, and deleted or returned to the submitting source.

3. STTAS Components will delete information or return it to the source, unless it is validated, every five (5) years, in accordance with 28 CFR Part 23.

4. 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 (2) above.

5. 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.

6. A record of information to be reviewed for retention will be maintained by the component, 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.

SAR Information Retention and Destruction

1. 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.

Accountability and Enforcement

Information System Transparency

(a) The policy establishing protections of privacy, civil rights, and civil liberties will be made available to the public on request and through any public web sites providing information about the system.

(b) Each component will designate an individual who is responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system. Cal EMA will post contact information on its website. In most instances, this should be the same individual designated as the Privacy Officer.

Accountability for Activities

(a) Primary responsibility for the operation of the STTAC 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. Each Component will make its own determination about the specific individual or position within its center that is most appropriate to fulfill this responsibility.

(b) STTAS Components 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) STTAS Components 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.

(d) STTAS Components will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users and the system itself with the provisions of this policy and applicable law.

(e) STTAS Components will require any individuals authorized to use the system to agree in writing to comply with the provisions of this policy. Each center will provide a printed copy of this policy to all agency and nonagency 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.

(f) STTAS Components will periodically conduct audits and inspections of the information contained in its information systems. The audits will be conducted randomly by a designated representative of the agency or by a designated independent party. The audit will be conducted in such a manner so as to protect the confidentiality, sensitivity, and privacy of the agency's information.

(g) STTAS Components will periodically review and update the provisions protecting privacy, civil rights, and civil liberties in its policies and make appropriate changes in response to changes in applicable law and public expectations.

Inadvertent Disclosure

(a) The STTAC shall disclose any breach of the security of a State of California system involving personal data following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) With regard to computerized data that includes personal information that the STTAC does not own, component 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 STTAC 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 agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency 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 California 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.
5. Health insurance information.

(f) (1) 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. (2) 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. (3) 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.

(g) 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.
3. Substitute notice, if the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the STTAC does not have sufficient contact information. Substitute notice shall consist of all of the following:

    (A) E-mail notice when the agency has an e-mail address for the subject persons.
    (B) Conspicuous posting of the notice on the agency's Web site page, if the agency maintains one.
    (C) Notification to major statewide media.

Enforcement

If a user is suspected of or found to be not complying with the provisions of this policy regarding the collection, use, retention, destruction, sharing, classification, or disclosure of information, the STTAS Component will take appropriate action based on the facts and circumstances of the specific incident. These include the following:

(a) Suspend or discontinue access to information by the user;
(b) Suspend, demote, transfer, or terminate the person as permitted by applicable personnel policies;
(c) Apply other sanctions or administrative actions as provided in agency personnel policies;
(d) Request the agency, organization, contractor, or service provider employing the user to initiate proceedings to discipline the user or enforce the policy’s provisions; or
(e) Refer the matter to appropriate authorities for criminal prosecution, as necessary and appropriate, to effectuate the purposes of the policy.

Training

(a) STTAS Components will require the following individuals to participate in training programs regarding the implementation of and adherence to the privacy, civil rights, and civil liberties policy:

1. Component employees, contractors, and consultants;
2. Personnel providing information technology services to the agency;
3. Staff in other public agencies or private contractors providing services to the agency; and
4. Users who are not employed by the agency or a contractor.

(b) The training program will cover:

1. Purposes of the privacy, civil rights, and civil liberties protection 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 agency;
3. The impact of improper activities associated with information accessible within or through the agency; and
4. The nature and possible penalties for policy violations, including possible transfer, dismissal, civil and criminal liability, and immunity, if any**.**

(c) STTAS Components will provide training to personnel authorized to share protected information in the ISE or e-Guardian. All reasonable efforts will be made to coordinate training efforts among the STTAS Components, where appropriate, to maximize the opportunity for training.

GOVERNANCE AND OVERSIGHT

The California State Terrorism Threat Assessment System (STTAS) Strategic Business Plan Concept of Operations (STTAS CONOPS) provides an overview of the five fusion center that comprise the STTAS. The governance structure and oversight mechanisms applicable to each STTAS Component are distinct and specific to a particular center.

Each STTAS Component 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 center adheres to this policy and the provisions of the Information Sharing Environment Privacy Guidelines. The Commander of each STTAS Component has been involved in the development of this policy and will retain responsibility for ensuring that it is rigorously implemented and refined as necessary. Each Commander, or his or her designee, is responsible for establishing and implementing appropriate procedures for resolving complaints involving SAR information. Each 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. STTAS Components will collaborate to ensure that best practices and training opportunities are made available to each Component to incorporate into its specific program as appropriate.

Definitions

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).*

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.

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.

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*.

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 Organization 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 482(f)(1) of the Homeland Security Act, homeland security information means any information possessed by a federal, state, local, or tribal
agency that relates to (A) a threat of terrorist activity; (B) the ability to prevent, interdict, or disrupt terrorist activity; (C) the identification or investigation of a suspected terrorist or terrorist organization or any person, group, or entity associated with or assisting a suspected terrorist or terrorist organization; or (D) a planned or actual response to a terrorist act.

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:

- Within a reasonable time;
- At a charge, if any, that is not excessive;
- In a reasonable manner; and
- 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.

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.

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.*

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.

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:

- Personal characteristics (such as height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation, place of birth, mother's maiden name, distinguishing features, and biometrics information, such as fingerprints, DNA, and retinal scans).

- A unique set of numbers or characters assigned to a specific individual (including name, address, phone number, social security number, e-mail address, driver's license number, financial account or credit card number and associated PIN number, Automated Integrated Fingerprint Identification System [AIFIS] identifier, or booking or detention system number).

- Descriptions of event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records).

- Descriptions of location(s) or place(s) (including geographic information systems [GIS] locations, electronic bracelet monitoring information, etc.).

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 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
Public includes:

- Any person and any for-profit or nonprofit entity, organization, or association;
- Any governmental entity for which there is no existing specific law authorizing access to the agency's information;
- Media organizations; and
- Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the agency.

Public does not include:

- Employees of the agency;
- People or entities, private or governmental, who assist the agency in the operation of the justice information system, and agency in the operation of the justice information system; and
- 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 Organization 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.

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.

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.

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 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.

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*.