Mission Statement

The Hawaii State Fusion Center (HSFC) is a partnership of law enforcement, first responders, and community stakeholders designed to appropriately collect, analyze, and disseminate information to enhance the protection of Hawaii's citizens, communities, and critical infrastructure.

I. Purpose

HSFC Information Privacy Policy ("Privacy Policy") establishes guidelines and procedures for the roles and responsibilities of HSFC staff and partners, to include users of the criminal intelligence system and other HSFC-maintained technology systems, regarding the manner in which information is collected, handled, stored, accessed, disseminated and purged within HSFC, as well as with other participating agencies and stakeholders in order to enforce strict protection of the privacy, civil rights, and civil liberties enjoyed by United States citizens under federal and state law.

II. Policy Applicability and Legal Compliance

This Privacy Policy applies to all information about individuals and organizations collected by HSFC in furtherance of its analytical mission. In adopting this Privacy Policy, HSFC shall implement it as an internal operating policy, along with other necessary policies, in a manner consistent with the state and federal law listed in Appendix B. The desired outcome of this policy is to enforce strict protection of the privacy rights, civil rights, and civil liberties enjoyed by U.S. citizens under federal and state law.

A. HSFC, 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.***

B. All HSFC users including all HSFC assigned or detailed personnel, information technology service providers, private contractors, agencies participating in the Information Sharing Environment (ISE) and other authorized participants in any HSFC operational component, shall comply with this Privacy Policy and all applicable laws protecting privacy, civil rights, and civil liberties, including those cited in Appendix B, in the collection, use, analysis, retention, destruction, sharing, and disclosure of information. The operating policies of each of HSFC's operational components will be consistent with this Privacy Policy and will

incorporate applicable laws protecting privacy, civil rights, and civil liberties. Violations of this section will be handled as outlined in Section XIV Accountability and Enforcement.

C. HSFC will provide a printed or electronic copy of this policy to all center and non-center personnel who provide services and will require both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and the applicable provisions it contains.

D. This Privacy Policy will be posted on the Office of Homeland Security Hawaii State Fusion Center Homeland Security Information Network Community of Interest.

III. Governance and Oversight

A. On June 25, 2013, Governor Neil Abercrombie signed Act 175 establishing the Office of Homeland Security within the State Department of Defense.

B. The Department of Defense shall be headed a single executive known as the adjutant general. The adjutant general shall be the director of the homeland security.

C. Primary responsibility for the day-to-day oversight is the Director of the HSFC and is responsible for its justice systems, operations, and coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing, disclosure, and dissemination of information.

D. The HSFC Director will designate a trained privacy officer. The Privacy Officer receives reports regarding alleged errors and violations of the provisions of this policy, receives and coordinates complaint resolution under the center's redress policy, and serves as the liaison for the ISE, ensuring that privacy protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy-enhancing technologies. The Privacy Officer can be contacted at the following address: 500 Ala Moana Blvd., Suite 5-200, Honolulu, HI, 96813

E. HSFC's Privacy Officer ensures that enforcement procedures and sanctions outlined in section XIV Accountability and Enforcement, Enforcement are adequate and enforced

IV. Definitions

See Appendix A: Glossary of Terms and Definitions

V. Information

A. HSFC will seek, or collect, information (to include placing information in criminal intelligence files) that:

1. ***Is based on a criminal predicate or possible threat to public safety***;
2. ***Is based on reasonable suspicion*** that an identifiable individual or organization has committed or is supporting or facilitating a criminal offense or is involved in or is

planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, Hawaii, or the nation, and that the information is relevant to the criminal (including terrorist) conduct or activity;
3. Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime;
4. Is useful in a crime or threat analysis or in the administration of criminal justice and public safety;
5. The source of the information is reliable and verifiable, or limitations on the quality of the information are identified; and/or
6. The information was collected in a fair and lawful manner, with the knowledge and consent of the individual, if appropriate.

B. HSFC may retain protected information that is based on a level of suspicion that is less than "reasonable suspicion", such as tips and leads or suspicious activity report (SAR) information, subject to the policies and procedures specified in subsections H and I.

C. HSFC ***will not*** seek or retain, and information-originating agencies will agree not to submit, information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, or sexual orientations.

D. The HSFC applies labels to entity-originated information (or ensures that the originating entity has applied labels) to indicate to the accessing authorized user that:

1. The information is "protected information", to include "personal data" on any individual (see Glossary) and, to the extent expressly provided in this policy, includes organizational entities.
2. The information is subject to laws (in Appendix B) restricting access, use, or disclosure.

E. HSFC personnel will, upon receipt of information, assess the information to determine its nature, usability, and quality. Personnel will assign categories to the information (or ensure that the originating agency will assign categories to the information) to reflect the assessment, such as:

1. Whether the information consists of tips and leads data, suspicious activity report (SAR) information, criminal history, intelligence information, case records, conditions of supervision, case progress, or Protected Critical Infrastructure Information (PCII), etc.;
2. The nature of the source as it affects veracity (e.g., anonymous tip, trained interviewer or investigator, public record, private sector, etc.);
3. The reliability of the source (i.e., reliable, usually reliable, unreliable, unknown);
4. The validity of the content (i.e., confirmed, probable, doubtful, cannot be judged);
5. The completeness of the information provided; and
6. The relevance and timeliness of the information, in regards to the date its accuracy was last verified, as well as whether or not the information is still applicable.

F. 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.

G. At the time a decision is made to retain information, it will be labeled, to the maximum extent feasible, pursuant to applicable limitations on access and sensitivity of disclosure to:

1. Protect confidential sources and police undercover techniques and methods;
2. Not interfere with or compromise pending criminal investigations;
3. Protect an individual's right of privacy, civil rights and civil liberties; and
4. Provide legally required protection based on the status of an individual as a victim or witness, as a child sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.

H. The classification of existing information will be reevaluated whenever:
1. New information is added that has an impact on access limitations or the sensitivity of disclosure of the information; or
2. There is a change in the use of the information affecting access or disclosure limitations (e.g., the information becomes part of court proceedings for which there are different public access laws).

I. HSFC personnel are required to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of ***tips and leads and suspicious activity report (SAR) information***. HSFC personnel will:

1. Prior to allowing access to or dissemination of the information, ensure that attempts to validate or refute the information have taken place and that the information has been assessed for sensitivity and confidence by subjecting it to an evaluation or screening process to determine its credibility and value, and categorize the information as unsubstantiated or uncorroborated if attempts to validate or determine the reliability of the information have been unsuccessful.
2. Store the information using the same storage method used for data that rises to the level of reasonable suspicion and includes an audit and inspection process, supporting documentation, and labeling of the data to distinguish it from other information.
3. Allow access to or disseminate the information using the same (or a more restrictive) access or dissemination method that is used for data that rises to the level of reasonable suspicion (e.g., "need-to-know" and "right-to-know" access or dissemination).
4. Regularly provide access to or disseminate the information in response to an interagency inquiry for law enforcement, homeland security, or public safety and analytical purposes, or provide an assessment of the information to any agency, entity, individual, or the public when credible information indicates potential imminent danger to life or property.
5. Retain information no longer than 120 days to work a tip or lead or SAR information to determine its credibility and value, assign a "disposition" label (for example, undetermined or unresolved, cleared or unfounded, or under active investigation) so that a subsequently authorized user knows that status and purpose for the retention

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

6. Adhere to and follow HSFC's physical, administrative, and technical security measures that are in place for the protection and security of tips and leads information. Tips, leads, and suspicious activity reports will be secured in a system that is the same or similar to the system that secures data that rises to the level of reasonable suspicion.
7. If the information collected rises to the level of reasonable suspicion/criminal predicate, the information may be retained/transferred into a system external to HSFC intelligence system if the system meets 28 CFR Part 23 compliance.

J. HSFC will incorporate the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious activities and incidents (SAR process) into existing processes and systems used to manage other crime-related information and criminal intelligence, thus leveraging existing policies and protocols utilized to protect the information, as well as constitutional rights, including personal privacy and other civil rights and civil liberties.

K. HSFC will ensure that SAR and ISE-SAR information posted in an external repository, such as RISS ATIX and e-Guardian will be subject to continuing assessment for confidence by subjecting it to an evaluation or screening process to confirm its credibility and value or categorize the information as unfounded or uncorroborated. Information determined to be unfounded will be purged.

L. Due diligence will be exercised in determining source reliability and content validity.

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

N. HSFC requires certain basic descriptive information to be entered and electronically associated with data (or content) that is to be accessed, used, and disclosed, including:

1. The name of the originating department, component, and subcomponent.
2. The name of the agency's justice information system from which the information is disseminated.
3. The date the information was collected, and where feasible, the date its accuracy was last verified.
4. The title and contact information for the person to who questions regarding the information should be directed.
5. Articulation of reasonable suspicion/criminal predicate for collecting and retaining the information.

O. HSFC 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.

P. HSFC shall keep a record of the source of information retained by the Center. In this context, "source" refers to the individual or entity which provided the information to HSFC. 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.

Q. The HSFC Director shall review all information and approve or deny its retention within a HSFC intelligence product file system based upon the following:

1. The information meets all requirements of this privacy policy; and
2. The source clearly defined reasonable suspicion/criminal predicate for the collection and retention of the information.

VI. Acquiring and Receiving Information

A. Information gathering (acquisition and access) and investigative techniques used by HSFC and information-originating agencies shall be in compliance with, and will adhere to, applicable regulations and guidelines, including, but not limited to:

1. 28 CFR Part 23 regarding criminal intelligence information;
2. Organization for Economic Co-operation and Development's (OECD) Fair Information Practices (under certain circumstances, there may be exceptions to the Fair Information Practices, based, for example, on authorities paralleling those provided in the federal Privacy Act; state, local, and tribal laws; or HSFC policy);
3. Applicable criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) National Criminal Intelligence Sharing Plan (NCISP);
4. Best practices advised by Law Enforcement Intelligence Unit (LEIU) and International Association of Law Enforcement Intelligence Analysts (IALEIA); and
5. Applicable constitutional provisions, Hawaii code, and the applicable administrative rules, as well as any other regulations that apply to multijurisdictional intelligence databases (See Appendix B).

B. HSFC's SAR process provides for human review and vetting to ensure that information is both legally gathered and, where applicable, determined to have a potential terrorism nexus. Law enforcement officers and HSFC staff will be trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism.

C. HSFC SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved in activities that have been determined to be consistent with criminal activities associated with terrorism will be documented and shared through the ISE. These safeguards are intended to ensure that information that could violate civil rights and civil liberties (e.g., race, culture, religion, or political associations) will not be intentionally or inadvertently gathered, documented, processed, and shared.

D. Information gathering techniques used by HSFC will and those used by originating agencies should be the least intrusive means necessary in the particular circumstances to gather information it is authorized to seek or retain.

E. External agencies that access and share information with HSFC are governed by the laws and rules governing those individual agencies, as well as by applicable federal and state laws.

F. HSFC will contract only with commercial database entities that provide an assurance that their methods for gathering personally identifiable information comply with applicable local, state, tribal, territorial, and federal laws, statutes, and regulations and that these methods are not based on misleading information collection practices.

G. HSFC will not directly or indirectly receive, seek, accept, or retain information from:
   1. An individual or nongovernment information provider if HSFC 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 HSFC.
   2. An individual or nongovernmental entity who may or may not receive a fee or benefit for providing the information.

VII. Information Quality Assurance

A. The HSFC will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources of information, accurate, current/relevant, and complete, including the relevant context in which it was sought or received.

B. Prior to the time of retention in the system, the information will be labeled regarding its level of quality (accuracy, completeness, currency, and confidence (verifiable and reliable)) by HSFC personnel and/or the submitting participant.

C. The labeling of retained information will be reevaluated when new information is gathered that has an impact on HSFC confidence in the validity or reliability of retained information.

D. HSFC will actively research suspected errors and deficiencies and will make every reasonable effort to ensure that information will be corrected or deleted from the system when:
   1. The information is erroneous, misleading, obsolete, or otherwise unreliable;
   2. The source of the information did not have authority to gather the information or to provide the information to HSFC; or
   3. The source of the information used prohibited means to gather the information, except when the source did not act as an agent to a bona fide law enforcement officer.

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

F. HSFC shall notify, in writing or electronic communication, recipient agencies if information provided by HSFC 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.

VIII. Collation and Analysis of Information

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

B. Information subject to collation and analysis is information as defined and identified in Section V.

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

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

- Provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal (including terrorist) activities.

IX. Merging of Records

Ownership of records remains with the originating agencies; as such, HSFC personnel will not merge records.

X. Sharing and Disclosure

A. Credentialed, role-based access criteria will be used, as appropriate, to control:
1. The information to which a particular group or class of users can have access based on the group or class;
2. The information a class of users can add, change, delete, or print; and
3. To whom, individually, the information can be disclosed and under what circumstances.

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

C. Access to or disclosure of records retained by HSFC will be provided ***only to persons within HSFC or in other governmental agencies*** who are authorized to have access and who have a legitimate law enforcement, public protection, public prosecution, public health or justice purpose. 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.

D. Records retained by HSFC may be accessed or disseminated ***to those responsible for public protection, safety, or public health*** only for public protection, safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures. An audit trail will be kept of access by or dissemination of information to such persons.

E. Information gathered and records retained by HSFC 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 of access by or dissemination of information to such persons.

F. Agencies external to the HSFC may not disseminate information accessed or disseminated from the center without approval from the center or other originator of the information.

G. Information gathered and records retained by HSFC will not be:
   1. Sold, published, exchanged, or disclosed for commercial purposes;
   2. Disclosed or published without prior notice to the contributing agency that such information is subject to re-disclosure or publication; or
   3. Disseminated to unauthorized persons.

H. HSFC provides intelligence analytical services to originating agencies only. This information is subject to 28 CFR Part 23, as such will not be disclosed to a member of the public. Requests for information will be referred to the originating agency. An audit trail will be kept of all requests and of what information is disclosed to a member of the public.

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

XI. Redress

A. Disclosure

1. HSFC provides intelligence analytical services to originating agencies only. This information is subject to 28 CFR Part 23, as such will not be disclosed to a member of the public. Requests for information will be referred to the originating agency. An audit trail will be kept of all requests and of what information is disclosed to a member of the public.

2. The existence, content, and source of the information will not be made available to an individual when:
   a. Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution;
   b. Disclosure would endanger the health or safety of an individual, organization, or community;

c. The information is in a criminal intelligence system subject to 28 CFR Part 23;
d. The information source does not reside with the HSFC; or
e. The HSFC did not originate, or does not otherwise have a right to disclose, the information.

B. Corrections

HSFC provides analytical services to originating agencies only. Individuals who submit requests for corrections will be referred to the originating agency. An audit trail will be kept of all requests and of what information is disclosed to a member of the public.

C. Appeals

HSFC provides analytical services to originating agencies only. Individuals who submit requests for corrections will be referred to the originating agency. The originating agency will be responsible for providing the procedure for appeals.

D. Complaints

1. To delineate protected information shared through the ISE from other data, HSFC maintains records of the ISE participating agencies to which the center has access, as well as audit logs, and employs system mechanisms whereby the source (or originating agency, including ISE participating agencies) is identified within the information.

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

The center will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the center's Privacy Officer at the following address: 500 Ala Moana Blvd., Suite 5-200, Honolulu, HI, 96813. The Privacy Officer will acknowledge the complaint and state that it will be reviewed but will not confirm the existence or nonexistence of the information to the complainant unless otherwise required by law. If the information did not originate with the center, the Privacy Officer will notify the originating agency in writing or electronically within 10 days and, upon request, assist such agency to correct any identified data/record deficiencies, purge the information, or verify that the record is accurate. All information held by the center that is the subject of a complaint will be reviewed within 30 days and confirmed or corrected/purged if determined to be inaccurate or incomplete, to include incorrectly merged information, or to be out of date. If there is no resolution within 30 days, the center will not share the information until such time as the complaint has been resolved. A record will be kept by the center of all complaints and the resulting action taken in response to the complaint.

XII. Security Safeguards

A. The HSFC Manager will be designated and trained to serve as the HSFC Security Officer.

B. HSFC will operate in a secure facility protecting the facility from external intrusion. HSFC will utilize secure internal and external safeguards against network intrusions. Access to HFSC databases from outside the facility will only be allowed over secure networks.

C. HSFC 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.

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

E. Access to HSFC information will only be granted to HSFC personnel and partners whose position and job duties require such access; who have successfully completed a background check and appropriate security clearance, if applicable, and have been selected, approved, and trained accordingly.

F. Queries made to HSFC data applications will be logged into each respective data system identifying the user initiating the query, as well as the date and time of the query whenever possible.

G. HSFC will utilize record logs to maintain audit trails of requested, sought and collected, and disseminated information. An audit trail will be kept for a minimum of one year of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.

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

I. HSFC 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 to investigate the release or any measures necessary to determine the scope of the release of information and, if necessary, to reasonably restore the integrity of any information system affected by this release.

J. With regard to computerized data that includes personal information that HSFC does not own, HSFC 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.

XIII. Information Retention and Destruction

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

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

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

D. Permission to destroy or return information or records will be presumed if the applicable information is not validated within the specified time period, as per item C. above.

E. A record of information to be reviewed for retention will be maintained by HSFC, 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.

XIV. Accountability and Enforcement

A. Information System Transparency:

1. HSFC will be open with the public in regard to information and intelligence collection practices. This Privacy Policy will be made available to the public on request and through the HSFC Web site: www.pacclear.org.

2. HSFC's Privacy Officer will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections. The Privacy Officer can be contacted at the following address: 500 Ala Moana Blvd., Suite 5-200, Honolulu, HI, 96813.

B. Accountability for Activities:

1. HSFC will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with their systems, in provisions of this policy and applicable law. This will include logging access of these systems and periodic and/or random auditing of these systems, so as to not establish a pattern of the audits. A record of the audit will be maintained by the Privacy Officer.

2. HSFC personnel or other authorized users shall report errors and suspected or confirmed violations of center policies relating to protected information to the Hawaii HIDTA/HSFC Director.

3. HSFC will annually and/or randomly conduct an audit and inspection of analytical products and intelligence contained in its information system(s). The audit will be conducted by an independent panel. This independent panel has the option of conducting a random audit, without announcement, at any time and without prior notice to staff of the center. The audit will be conducted in such a manner as to

protect the confidentiality, sensitivity, and privacy of the center's information and intelligence system(s).

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

C. Enforcement:

1. 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, HSFC will take appropriate action based on the facts and circumstances of the specific incident. These include the following:

   a. Counsel and/or re-train.
   b. Suspend or discontinue access to information by the user.
   c. Suspend, demote, or terminate contract employees as permitted by applicable HIDTA personnel policies;
   d. If the user is from an external agency, HSFC will return the individual to the parent agency and request that the relevant agency 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 this policy.

2. HSFC reserves the right to restrict the qualifications and number of personnel having access to HSFC information and to suspend or withhold service to any personnel violating this privacy policy. HSFC reserves the right to deny access to any participating agency user who fails to comply with the applicable restrictions and limitations of HSFC's privacy policy.

XV. Training

A. HSFC will require the following individuals to participate in training programs regarding the implementation of and adherence to this Privacy policy:
   1. All HSFC employees and full-time contractors and consultants;
   2. All HSFC Intelligence Liaison Officers (ILOs), and participating analysts;
   3. Personnel providing information technology services or other services to HSFC;
   4. Staff in other public or private agencies participating with HSFC.

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

C. HSFC's Privacy Policy training programs will cover:
   1. Purposes of the Privacy Policy;

2. Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by HSFC;
3. Originating and participating agency responsibilities and obligations under applicable law and policy;
4. How to implement the policy in the day-to-day work of the user, whether a paper or systems user;
5. The impact of improper activities associated with infractions within or through HSFC;
6. Mechanisms for reporting violations of HSFC's Privacy Policy; and
7. 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 ISE, access refers to the business rules, means, and processes by and through which ISE participants obtain terrorism-related information, to include homeland security information, terrorism information, and law enforcement information acquired in the first instance by another ISE participant

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

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

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

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

Authentication - Authentication is the process of validating the credentials of a person, computer process, or device. Authentication requires that the person, process, or device making the request provide a credential that proves it is what or who it says it is. Common forms of credentials are digital certificates, digital signatures, smart cards, biometrics data, and a combination of user names and passwords. See Biometrics.

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

Breach of the security of the system - 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 HSFC. Good faith acquisition of personal information by an employee or partner of HSFC for the purposes of HSFC 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.

Center - "Center" refers to the Statewide Information & Analysis Center and all participating state agencies of the Statewide Information & Analysis Center.

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

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

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

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

Criminal Intelligence Information or Data - Information deemed relevant to the identification of and the criminal activity engaged in by an individual who or organization that is reasonably suspected of involvement in criminal acts. The record is maintained in a criminal intelligence system per 28 CFR Part 23. Reasonable suspicion/criminal predicate applies to the information. The record is maintained per 28 CFR Part 23.

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

Criminal Predicate **-** See *Reasonable Suspicion.*

Data **-** Inert symbols, signs, descriptions, or measures.

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

Data Quality Principle **-** One of the eight Fair Information Principles (FIPs) developed by the Organization 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 Organization 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

Health insurance information - 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.

Homeland Security Information - As defined in Section 892(f)(1) of the Homeland Security Act of 2002 and codified at 6 U.S.C. § 482(f)(1), homeland security information means any information possessed by a federal, state, or local agency that (a) relates to a threat of terrorist activity; (b) relates to the ability to

prevent, interdict, or disrupt terrorist activity; (c) would improve the identification or investigation of a suspected terrorist or terrorist organization; or (d) would improve the response to a terrorist act.

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

Individual Participation Principle **-** One of the eight Fair Information Principles (FIPs) developed by the Organization for Economic Co-operation and Development (OECD). As stated in the FIPs, according to this principle, an individual should have the right:

A. To obtain from the data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

B. To have communicated to him, data relating to him:
   1. Within a reasonable time;
   2. At a charge, if any, that is not excessive;
   3. In a reasonable manner; and
   4. In a form that is readily intelligible to him.

C. To be given reasons if a request made under subparagraphs a) and b) is denied, and to be able to challenge such denial; and

D. To challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed, or amended.

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

Furthermore, information is data that may include records, documents, or files pertaining to law enforcement operations, such as computer-aided dispatch (CAD) data, incident data, and management information; data that is maintained in a records management, CAD system, etc., for statistical/retrieval purposes. Information may be either resolved or unresolved. The record is maintained per statute, rule, or policy.

Information Disclosure **-** The exposure of information to individuals who normally would not have access to it.

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

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

Information Sharing Environment (ISE) **-** In accordance with Section 1016 of the Intelligence Reform and Terrorism Prevention Act (IRTPA), as amended, the ISE will be composed of policies, procedures, and technologies linking the resources (people, systems, databases, and information) of state, local, and tribal (SLT) and federal entities and the private sector to facilitate terrorism information sharing, access, and collaboration. Consistent with Presidential Guideline 5, the U.S. Attorney General, the U.S. Department of Justice (DOJ), and the Director of National Intelligence (DNI)—in coordination with the Program Manager for the ISE (PM-ISE) and the heads of federal departments and agencies that possess or use intelligence or other terrorism-related information—developed privacy guidelines for the ISE, titled Guidelines to Ensure That the Information Privacy and Other Legal Rights of Americans Are Protected in the Development and Use of the Information Sharing Environment (ISE Privacy Guidelines). The ISE Privacy Guidelines describe the means by which federal departments and agencies participating in the ISE will protect privacy and civil liberties in the development and operation of the ISE.

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

Intelligence System **-** See *Criminal Intelligence System*.

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

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

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

Law Enforcement Information **-** For purposes of the ISE, law enforcement information means any information obtained by or of interest to a law enforcement agency or official that is both (a) related to

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

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

Maintenance of Information - The maintenance of information applies to all forms of information storage. This includes electronic systems (for example, databases) and non-electronic storage systems (for example, filing cabinets). To meet access requirements, an organization is not required to create new systems to maintain information or to maintain information beyond a time when it no longer serves an organization's purpose.

Medical information - 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.

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.

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

Notice - 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 forth in Section 7001 of Title 15 of the United States Code; or
C. Substitute notice, if the cost of providing notice is deemed "excessive", or HSFC does not have sufficient contact information. Substitute notice shall consist of all of the following:
    - E-mail notice when HSFC has an e-mail address for the subject person(s);
    - Conspicuous posting of the notice on HSFC/s web site; or
    - Notification to major statewide media.

Openness Principle - One of the eight Fair Information Principles (FIPs) developed by the Organization for Economic Co-operation and Development (OECD). According to this principle, there should be a general policy of openness about developments, practices, and policies with respect to personal data. Means

should be readily available for establishing the existence and nature of personal data and the main purposes of their use, as well as the identity and usual residence of the data controller.

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

Personal Information - See *Personally Identifiable Information*.

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

A. Personal characteristics (such as height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation, place of birth, mother's maiden name, distinguishing features, and biometrics information, such as fingerprints, DNA, and retinal scans).
B. A unique set of numbers or characters assigned to a specific individual (including name, address, phone number, social security number, e-mail address, driver's license number, financial account or credit card number and associated PIN number, Automated Integrated Fingerprint Identification System [AIFIS] identifier, or booking or detention system number).
C. Descriptions of event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records).
D. Descriptions of location(s) or place(s) (including geographic information systems [GIS] locations, electronic bracelet monitoring information, etc.).

Persons **-** Executive Order 12333 defines "United States persons" as United States citizens, aliens known by the intelligence agency concerned to be permanent resident aliens, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for
a corporation directed and controlled by a foreign government or governments. For the intelligence community and for domestic law enforcement agencies, "persons" means United States citizens and lawful permanent residents.

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

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

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

Protected Critical Infrastructure Information (PCII) Program - The Protected Critical Infrastructure Information (PCII) Program, established pursuant to the Critical Infrastructure Information Act of 2002 (CII Act), creates a framework which enables members of the private sector to voluntarily submit confidential information regarding the nation's critical infrastructure to the Department of Homeland Security (DHS) with the assurance that the information, if it satisfies the requirements of the CII Act, will be protected from public disclosure.

The PCII Program seeks to facilitate greater sharing of critical infrastructure information among the owners and operators of the critical infrastructures and government entities with infrastructure protection responsibilities, thereby reducing the nation's vulnerability to terrorism.

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

Public

A. Public includes:
    1. Any person and any for-profit or nonprofit entity, organization, or association;
    2. Any governmental entity for which there is no existing specific law authorizing access to the agency's information;
    3. Media organizations; and
    4. Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the agency.
B. Public does not include:
    1. Employees of the agency;
    2. People or entities, private or governmental, who assist the agency in the operation of the justice information system, and agency in the operation of the justice information system; and
    3. Public agencies whose authority to access information gathered and retained by the agency is specified in law.

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

Purpose Specification Principle - One of the eight Fair Information Principles (FIPs) developed by the 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.

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

Record - Any item, collection, or grouping of information that includes personally identifiable information and is maintained, collected, used, or disseminated by or for the collecting agency or organization.

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

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

Right to Know - Based on having legal authority or responsibility or pursuant to an authoriz3ed agreement, an agency or organization is authorized to access sensitive information and intelligence in the performance of a law enforcement, homeland security, or counterterrorism activity.

Right to Privacy - The right to be left alone, in the absence of some reasonable public interest in gathering, retaining, and sharing information about a person's activities. Invasion of the right to privacy can be the basis for a lawsuit for damages against the person or entity violating a person's privacy.

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

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

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

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

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

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

A. Storage is frequently used to mean the devices and data connected to the computer through input/output operations—that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-computer storage. This meaning is probably more common in the IT industry than meaning B.

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

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

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

Suspicious Activity **-** Suspicious activity is defined as "reported or observed activity and/or behavior that, based on an officer's training and experience, is believed to be indicative of intelligence gathering or preoperational planning related to terrorism, criminal, or other illicit intention." Examples of suspicious activity include surveillance, photography of facilities, site breach or physical intrusion, cyberattacks, testing of security, etc.

Suspicious Activity Report (SAR) Information **-** The observation and documentation of a suspicious activity. At the federal level, there are two types of SAR information: 1) Information Sharing Environment SAR information that pertains to terrorism information; and 2) Banking Secrecy Act SAR information that pertains to suspicious banking activity and is required to be completed by financial institutions. 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, the state-designated fusion center. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor are they designed to support interagency calls for service.

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

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

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

Tips and Leads Information or Data **-** Uncorroborated report or information generated from inside or outside the agency that alleges or indicates some form of possible criminal activity. Tips and leads can also be referred to as suspicious incident report (SIR) information, suspicious activity report (SAR) information, and/or field interview reports (FIRs). Tips and leads information does not include incidents that do not have an offense attached, criminal history records, or CAD data. Tips and leads information is maintained in a secure system, similar to data that rises to the level of reasonable suspicion.

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

Transborder Flows of Personal Data **-** Movements of personal data across national borders. See *Fair Information Principles (FIPs)*.

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

Use Limitation Principle **-** One of the eight Fair Information Principles (FIPs) developed by the Organization 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*.

Appendix B: Applicable State and Federal Law

Hawaii State Law

Act 175 Office of Homeland Security
Hawaii Constitution, August 21, 1959
Hawaii Revised Statutes (HRS) 92F (Uniform Information Practices Act)
HRS 286-171 and 286-172 (Traffic Records)
HRS 291C (Statewide Traffic Code)
HRS 353 (Corrections)
HRS 487J (Social Security Number Protection)
HRS 487N (Security Breach of Personal Information
HRS 571 (Family Courts)
HRS 846D (Juvenile Justice Information System)

Federal Law

Federal Code 28USC 534 (FBI Identification Records and Information)
Access to Classified Information, Presidential Executive Order 12968, August 4, 19954
Audits of States, Local Governments, and Non-Profit Organizations, OMB Circular A-133, (Single Audit Act), revised June 27, 2003 and June 26, 2007
Bank Secrecy Act, 31 U.S.C. §5311, United States Code, Title 31, Subtitle IV, Chapter 53, Subchapter 11, §5311, and 31 CFR §103
Cost Principles for State, Local, and Indian Tribal Governments, OMB Circular A-87, revised May 10, 2004
Government Performance and Results Act of 1993 (GPRA), Public Law 103-62, 103rd Congress, August 3, 1993
Grants and Cooperative Agreements with the State and Local governments, OMB Circular A-102, (Common rule), revised August 29, 1997
Violent Crime Control and Law Enforcement Act, Public Law 103-322, 103rd Congress, September 13, 1994
28 CFR Part 23