Connecticut Intelligence Center
Privacy, Civil Rights, and Civil Liberties
Protection Policy

November19, 2010 Version 1.0 Sent to DHS Privacy Officer with IIRDHS Recommendation for Approval and Approved by DHS Privacy Office by Letter dated December 1, 2010

A. Purpose Statement

The purpose of the Connecticut Intelligence Center (CTIC) is to collect, evaluate, analyze, and disseminate information and intelligence data (records) regarding criminal and terrorist activity relevant to Connecticut while following the ***Fair Information Practices*** to ensure the rights and privacy of citizens.

The purpose of this privacy, civil rights, and civil liberties policy is to promote CTIC agency and user conduct, including conduct related to Suspicious Activity Reports (SAR), that complies with applicable laws and assists CTIC and its users in:

- Protecting individual privacy, civil rights, civil liberties, and other protected interests;
- Increasing public safety and improving national security;
- Minimizing the threat and risk of injury to specific individuals;
- Minimizing the threat and risk of injury to law enforcement and others responsible for public protection, safety, or health;
- Minimizing the threat and risk of damage to real or personal property;
- Protecting the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information;
- Encouraging individuals or community groups to trust and cooperate with the justice system;
- Supporting the role of the justice system in society;
- Promoting governmental legitimacy and accountability;
- Making the most effective use of public resources allocated to public safety agencies.

B. Policy Applicability and Legal Compliance

1. All CTIC personnel, participating agency personnel, personnel providing information technology services to CTIC, private contractors, and other users

authorized by the Director of CTIC and the CTIC Security Officer (hereafter "CTIC Authorized Users") will comply with CTIC's privacy policy. This policy applies to information that CTIC gathers or collects, receives, maintains, stores, accesses, discloses, or disseminates to CTIC personnel, governmental agencies (including Information Sharing Environment [ISE] participating centers and agencies), and participating justice and public safety agencies, as well as to private contractors, private entities, and the general public.

2. The CTIC will provide a printed or electronic copy of this policy to all CTIC Authorized Users and participating agencies and will require both a written acknowledgement of receipt of this policy and a signed agreement to comply with this policy.

3. All CTIC personnel, other Authorized Users, agencies that originate information, and any other users are to comply as required with applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to:

   - United States Constitution and United States Constitutional Amendments I-XXVII
   - The Privacy Act of 1974 (5 U.S.C. 552a)
   - United States Executive Order 12958 "Classified National Security Information"
   - United States Department of Justice Criminal Intelligence Systems Operating Policies: 28 CFR Part 23 (1993)
   - Connecticut Statutory Provisions With an Impact on the Disclosure of Records (See Appendix B)
   - Connecticut Constitution and Amendments

4. CTIC's internal operating policies are to comply as required with applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to, State and Federal privacy, civil rights, and civil liberties laws, statutes and regulations, cited in Appendices B and C, as amended from time to time (See, for example, the partial listing of nondisclosure laws in Appendix B).

C. Governance and Oversight

1. Primary responsibility for the operation of the CTIC; its justice systems, operations, and coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing, disclosure, or dissemination of information; and the enforcement of this policy is assigned to the CTIC Director.

2. CTIC has designated trained Privacy and Security Officers. The Privacy Officer and the Security Officer, consulting with a CTIC Legal Working Group made up of

legal representatives from CTIC participating agencies, will receive and review any allegations regarding violations of this policy, and report findings to the CTIC Director. An annual privacy policy review will be conducted by this group each January, with a report, including recommendations on possible updates to the policy, to be submitted to the CTIC Director by March 30''.

3. The Privacy and Security Officers are the liaisons to citizen and community privacy advocacy groups to ensure that privacy, civil rights and civil liberties are protected within the parameters of this policy and within CTIC's information collection, retention, and dissemination processes and procedures. They serve as liaisons for the Information Sharing Environment, to ensure that privacy protections are implemented through such efforts as training, process, and system designs. The Attorney for the Connecticut Department of Emergency Management and Homeland Security serves as the CTIC Privacy Officer. The Privacy Officer receives reports regarding alleged errors and violations of the provisions of this policy, and receives and coordinates complaint resolution under the CTIC redress policy. The Privacy Officer can be contacted at the following address: CTIC Privacy Officer, Department of Emergency Management and Homeland Security, 25 Sigourney Street, Hartford, CT 06106 or by e-mail at ctic.privacyofficer@ct.gov.

4. CTIC's Director, working with the Privacy Officer, ensures that enforcement procedures and sanctions outlined in Section N.3 are adequate and enforced.

D. Definitions

For primary terms and definitions used in this policy, please see Appendix A, Terms and Definitions.

E. Information

1. The CTIC will comply with all applicable laws and regulations in seeking, retaining, and distributing information.

2. a) The CTIC will collect/receive and retain as appropriate ''personally identifiable information,'' as defined in Appendix **A,** where such information is based on reasonable suspicion that the identifiable individual has committed a criminal offense or is involved in or planning criminal or terrorist activity.

   b) Subject to the other provisions contained in Section E, CTIC will retain ''protected information'' that does not rise to the level of reasonable suspicion for a maximum of 15 months to allow the law enforcement and intelligence community to attempt to corroborate or otherwise verify the accuracy of that information and its relevance to any criminal or terrorist activity. Conn. Gen Stat. § 1-216.

c) Reasonable Suspicion is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, employee, or intelligence analyst a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal or terrorist activity or enterprise. **28** C.F.R. Part **23.**

d) The retention period for a particular document may be affected by court order in certain cases.

3. At the time a decision is made by the CTIC to retain information, it will be evaluated to the maximum extent feasible to:

- protect confidential sources and police undercover techniques and methods;
- not interfere with or compromise pending criminal investigations; and
- protect the privacy, civil rights, and civil liberties of all persons, including, but not limited to, legally required protections based on the 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.

4. In compliance with applicable privacy and civil liberties requirements, and with respect to sharing protected information, the CTIC will collect/receive and retain information, including "personally identifiable information," in a manner that:

- pertains to a possible violation of federal or state criminal laws or a threat to public safety; or
- is relevant to the investigation or prosecution of suspected criminal or terrorist incidents or the enforcement of sanctions, orders, or sentences related thereto; or
- is useful in crime analysis or in the administration of criminal justice and public safety.

5. The CTIC will not collect/receive or retain, and participating 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 non-criminal organization or lawful event; or their race, religious creed, age, marital status, national origin, ethnicity, color, ancestry, gender, citizenship, sexual orientation, or mental or physical disability. For similar language, see Connecticut General Statutes §§4a-60 and 4a-60a.

6. The CTIC will appropriately identify/label information that it distributes to indicate to the authorized user any privacy protections or other restrictions regarding the access, use, or disclosure of such information.

The CTIC applies labels to center-originated information (or ensures that the originating agency has applied labels) to indicate to the accessing authorized user that:

- The information is "protected information" as defined by CTIC (See Appendix A, Terms and Definitions);
- The information that CTIC distributes is subject to any state or federal privacy protections or other restrictions regarding the access, use or disclosure of such information (See Appendices B and C.)

7. CTIC personnel will, upon receipt of information, determine its nature, relevance and reliability. Personnel will assign categories to the information (or ensure that the originating agency has assigned categories to the information) to reflect:

- the reliability of the source, if known;
- the nature of the source, if known;
- the extent to which any such information has been corroborated;
- the degree of reliability that the originating agency ascribes to that information; and
- Whether the information consists of tips, leads, and data, suspicious activity reports, criminal history, intelligence information, conditions of supervision, or other information category.

8. The labeling/identification of existing CTIC information will be reevaluated when:

- new information is received that affects access limitations or the sensitivity of said information; or
- the nature of such information is affected, for example, by subsequent legal or court proceedings that affect its retention and distribution.

9. CTIC personnel will adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of "personally-identifiable information" that derives from tips, leads, or suspicious activity reports (SAR) that does not rise to the level of "reasonable suspicion":

- Prior to allowing access to or dissemination of the information, ensure that attempts to validate the information have taken place and ensure that the information has been assessed for sensitivity (dissemination) and confidence (source reliability and content validity) by subjecting it to an evaluation and screening process and categorize the information as unsubstantiated or uncorroborated if attempts to validate or determine the reliability of the information have been unsuccessful;

CTIC will use a standard reporting format and data collection codes for SAR information;

Store the information using the same storage method used for data which rises to the level of reasonable suspicion and includes an audit and inspection process, supporting documentation, and labeling of such data to differentiate it from other information;

Provide access to or disseminate such information in response to an interagency inquiry for law enforcement, homeland security, or public safety purposes when credible information indicates potential danger to life or property;

Allow access to or disseminate information using the same (or a more restrictive) access or dissemination standard that is used for data that rises to the level of reasonable suspicion (for example, "need-to-know" access or dissemination for personally identifiable information);

Retain such information for a period of 15 months in order to pursue tips, leads, or SAR information to determine its credibility and relevance to possible criminal or terrorist activity, in accordance with Connecticut General Statutes §1-216; and

Adhere to and follow the CTIC physical, administrative, and technical security measures to ensure protection and security of such information.

10. The CTIC incorporates terrorism-related SARs into existing processes and systems, thus leveraging existing policies and protocols utilized to protect the information as well as the privacy, civil rights, and civil liberties of all persons.

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

12. The CTIC requires certain basic descriptive information (metadata tags or labels) to be entered and electronically associated with data (or content) for which there are special laws, rules, or policies regarding access, use, and disclosure, including terrorism-related information shared through the ISE. The types of information include:

- The name of the originating center, department or agency, component, and subcomponent;

- The name of the center's justice information system from which the information is disseminated;

- The date the information was collected and, where feasible, the date its accuracy was last verified;

- The title and contact information for the person to whom questions regarding the information should be directed.

13. The CTIC will identify/label (or ensure that the originating agency has identifiedllabeled) any legal restrictions on information sharing based on information sensitivity or classification to information used, accessed, or disseminated.

14. The CTIC will keep a record of the source of all information sought and collected by the center.

F. Acquiring and Receiving Information

1. Information-collecting/receiving and access techniques used by CTIC and information-originating agencies, as well as investigative techniques by appropriate agencies, will remain in compliance with and will adhere to applicable laws and guidance, including, but not limited to:

    - 28 CFR Part 23, regarding criminal intelligence information;

    - The Organization for Economic Co-operation and Development's (OECD) Fair Information Principles;

    - Applicable criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) ***National Criminal Intelligence Sharing Plan*** (NCISP);

    - Applicable relevant Constitutional provisions, Connecticut General Statutes, and administrative rules, as well as regulations and policies that apply to multijurisdictional intelligence and information sharing [databases]. (See B-3, Policy Applicability and Legal Compliance: for example, Connecticut General Statutes §1-216 regarding uncorroborated information.)

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

3. The CTIC's SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved in activities that have been determined to be consistent with criminal activities associated with terrorism will be

documented and shared through the ISE. These safeguards are intended to ensure that information that could violate civil rights and/or civil liberties (for example, information based solely on race, color, religious creed, age, marital status, national origin, ancestry, gender, mental or physical disability) will not be intentionally or inadvertently gathered, documented, processed, and shared.

4. Information-gathering techniques used by CTIC will be the least intrusive means necessary in the particular circumstances to gather information it is authorized to seek or retain.

5. External agencies that access and share information with CTIC are governed by the laws and rules governing those individual agencies, including applicable federal and state laws.

6. CTIC will request that the Connecticut Department of Information Technology contract on its behalf only with commercial database entities that provide an assurance that their methods for gathering personally identifiable information comply with applicable law.

7. CTIC will not directly or indirectly knowingly receive, seek, accept, or retain information fiom any individual or information provider that is legally prohibited fiom obtaining or disclosing the information, except as allowed by law.

G. Information Quality Assurance

1. CTIC will make every reasonable effort to ensure that information collected/received or retained is derived fiom dependable and trustworthy sources; accurate; current; complete, including the relevant context in which it was collected or received; and merged with other information about the same individual or organization only when the applicable standard (See Section I, Merging Records) has been met.

2. At the time of retention in the system, the information will be evaluated/labeled regarding its level of quality (accuracy, completeness, currency, and reliability.)

3. CTIC will review, in a timely manner, alleged errors and deficiencies in information quality (or refer them to the originating agency) and will correct, delete, or refrain fiom using protected information found to be erroneous or deficient.

4. The labeling of retained information will be reevaluated by CTIC or the originating agency when new information is gathered that has an impact on the validity and reliability of previous information.

5. CTIC will conduct ongoing data quality reviews of information it originates and make reasonable efforts to ensure that information will be corrected, deleted fiom the system, or not used when CTIC learns that the information is erroneous, misleading, obsolete, or otherwise unreliable; the CTIC did not have authority to

gather the information or to provide the information to another agency; or the CTIC used prohibited means to gather the information.

6. Originating agencies external to CTIC are responsible for reviewing the quality and accuracy of the data provided to CTIC. CTIC will advise the originating agency's privacy official, if one exists, or that agency's contact person, in writing, if data is alleged, suspected, or found to be inaccurate, incomplete, or out of date.

7. CTIC will use reasonable efforts to provide written or electronic notification to inform recipient agencies when information previously provided to the recipient agency is deleted or changed by CTIC because the information is determined to be erroneous, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate content such that the rights of the individual may be affected.

H. Information Analysis

1. Information collected/received by CTIC or accessed from other sources will be analyzed only by selected, approved, and trained individuals who have successfully completed a background check and, if applicable, meet appropriate security clearance levels.

2. Information subject to analysis is identified in Section E.

3. Information collected or received by CTIC or accessed from other sources is analyzed according to Connecticut's Standing Information Needs (SINs) and will be analyzed to:

   - Prevent crime and terrorism, and further law enforcement, public safety, force deployment, or prosecution objectives and priorities established by CTIC;

   - 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 and terrorism activities; and

   - Promote appropriate information sharing.

I. Merging Records

1. Records about an individual or organization from two or more sources will not be merged by CTIC unless there is sufficient identifying information to reasonably conclude that the information is about the same individual or organization. The set of identifiers sufficient to allow merging will consist of all available attributes that can contribute to a higher accuracy of match.

2. If there is an identified partial match, the information may be associated by CTIC if accompanied by a clear statement that it has not been adequately established that the information relates to the same individual or organization.

J. Sharing and Disclosure

1. Credentialed, role-based access criteria will be used by CTIC, as appropriate, to control:

- The information to which a particular group or class of users can have access based on the group or class;
- The information a class of users can add, change, delete, or print; and,
- To whom, individually, the information can be disclosed and under what circumstances.

2. CTIC adheres to the current version of the ISE-SAR Functional Standard for the suspicious 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 reporting.

3. Access to or disclosure of records retained by CTIC will be provided only *to persons within CTIC or in other governmental agencies* who are authorized to have access and only for legitimate law enforcement, public protection, safety, public prosecution, public health, or justice purposes and only for the performance of official duties in accordance with law and procedures applicable to the agency for which the person is working.

An audit trail sufficient to allow the identification of each individual who accessed information retained by CTIC and the nature of the information accessed will be kept by CTIC.

4. Agencies and individuals may not disseminate information accessed or disseminated from CTIC without prior approval from CTIC or other originator of the information. If approval is received from originator of information other than CTIC, CTIC must be notified.

5. Records retained by the CTIC may be accessed by or disseminated ***to those responsible for public protection, public safety, or public health*** only for public protection, public safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures. An audit trail sufficient to allow the identification of each individual who accessed or received information retained by CTIC and the nature of the information accessed will be kept by CTIC. CTIC will not limit the dissemination of an assessment of information to a government official or to any other individual, organization, or entity when necessary to avoid imminent danger to life or property.

6. Information gathered or collected and records retained by CTIC may be accessed or disseminated ***for specific purposes*** and upon approval of the Security Officer upon request by persons authorized by law to have such access and only for those uses and purposes specified in the law. An audit trail sufficient to allow the identification of each individual who requested, accessed, or received information retained by CTIC; the nature of the information requested, accessed, or received; and the specific purpose will be kept for at least five years by CTIC.

7. Information gathered and records retained by CTIC may be accessed or 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, and is not exempt fiom disclosure by law. Such information may be disclosed only in accordance with the law and procedures applicable to CTIC for this type of information. An audit log will be kept of all requests and the information disclosed to the public.

8. Information gathered or collected and records retained by CTIC shall not be:

   - Sold, published, exchanged, or disclosed for commercial purposes by CTIC;
   - Disclosed or published without prior notice to the originating agency that such information is subject to disclosure or publication, unless disclosure is agreed to as part of the normal operation of the agency, or is required by law; or
   - Knowingly disseminated by CTIC to persons not authorized to access or use the information.

9. Federal and/or state law, or other legal instrument or order, may prohibit the disclosure of certain information to a member of the public. For examples of laws that may be applicable, see Appendices B and C. See for example, Connecticut General Statutes Section 1-210(b) for exemptions to the Connecticut Freedom of Information Act, and the National Security Act, Public Law 235, Section 606, in accord with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18,2010.

10. Unless otherwise required by law, CTIC shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information.

K. Redress

Requests from individuals for access to protected information; merged records; and complaints from individuals who believe that protected information about them is inaccurate or incomplete will be received by CTIC. Responses to such requests and/or complaints will be handled pursuant to this section.

1. Disclosure

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

Unless the requested information has originated with CTIC, CTIC will refer an individual's request for the opportunity to review protected information and/or merged record about him/herself to the originating agency. Within 90 days of any such review, the originating agency shall advise CTIC of what information, if any, was disclosed to the requestor or of any changes made to the information as a result of the originating agency's review.

Requested information originating from a CTIC system will be available upon satisfactory verification of the individual's identity, unless restricted by applicable law, or other legal authority. CTIC will respond to such a request for protected information and/or merged record within a reasonable time and in a form that is intelligible to the individual.

A record will be kept of all requests and of what protected information and/or merged record is disclosed to an individual, if known by CTIC.

The existence, content, and source of the information will not be made available by the CTIC to an individual when the information is exempt under the Connecticut Freedom of Information Act or other applicable state or federal law.

2. Corrections

If an individual requests correction of protected information and/or merged record ***originating with*** CTIC that has been disclosed, CTIC's Privacy Officer or designee will inform the individual of the procedure for requesting and considering requested corrections, including appeal rights if requests are denied in whole or in part. **A** record will be kept of all requests for corrections and the resulting action, if any.

3. Appeals

CTIC will advise any individual whose request for disclosure of information or request for correction of information is denied of the basis for the denial and the procedure of filing an appeal. If the information did not originate with CTIC, the individual may be referred to the originating agency as appropriate.

4. Complaints

If an individual has a complaint with regard to the accuracy or completeness of terrorism-related protected information that:

- Is exempt fiom disclosure,
- Has been or may be shared through the ISE,
- Is held by CTIC, and,
- Allegedly has resulted in demonstrable harm to the complainant,

CTIC will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the CTIC Privacy Officer at CTIC Privacy Officer, Connecticut Department of Emergency Management and Homeland Security, 25 Sigourney Street, Hartford, CT 06106, or by e-mail at **ctic.privacyofficer@ct.gov.** The Privacy Officer will acknowledge receipt of the complaint within ten business days, 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 CTIC, the Privacy Officer will notify the originating agency in writing or electronically within ten business 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 CTIC that is the subject of a complaint will be reviewed within 120 days and confirmed or corrected/purged if determined to be inaccurate or incomplete, to include incorrectly merged information, or to be out of date.

CTIC will use all reasonable efforts to resolve the complaint within 120 days. CTIC will generate and send a response to the email or mailing address provided by the complainant. If CTIC has not resolved the complaint within 120 days, CTIC will not share the information until such time as the complaint is resolved. CTIC will keep a record of all complaints and the resulting action taken in response to the complaint.

To delineate protected information shared through the ISE fiom other data, the CTIC maintains records of agencies sharing terrorism-related information and employs system mechanisms to identify the originating agency when the information is shared.

L. Security Safeguards

1. The CTIC Operations Supervisor is designated and trained to serve as the CTIC Security Officer.

2. The CTIC will operate in a secure facility protected from external intrusion. The center will utilize secure internal and external safeguards against network intrusions. Access to the center's databases from outside the facility will be allowed only over secure networks.

3. Access to the CTIC area is restricted to authorized personnel. Physical access to CTIC is supported by several layers of security including; 24 hour facility access controls. Visitors to CTIC must present proper identification and are escorted by an authorized CTIC employee at all times.

4. Technical safeguards to ensure security of data collected and stored by the CTIC are governed by Information Technology Policy and Standards set forth by the Connecticut Department of Information Technology (DOIT). Policies, architecture, standards and planning guidelines issued by DOIT are in accordance with Conn. Gen. Stat §4d-2(c).

5. Any situation or observation that affects the integrity of data stored physically or electronically, security vulnerabilities or any potential or known compromises of information or materials will be reported to the Security Officer.

6. The CTIC will secure SAR information in a separate repository on a secure server at an offsite location. Policies for access to this system are consistent with IT Policy and Standards set forth by the Connecticut Department of Information Technology (DOIT) in accordance with Conn. Gen. Stat. §4d-2(c).

7. The computer and communications system privileges of all users, systems, and operating programs will be restricted based on the need-to-know. All computers permanently or intermittently connected to State of Connecticut networks will employ password-based access controls. All users must be positively identified prior to being able to use any multi-user computer or communications system resources.

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

9. Access to CTIC information will be granted only to center personnel whose positions and job duties require such access; who have successfully completed a criminal background check and are eligible to receive a national security clearance at the level of SECRET and who have been selected, approved, and trained accordingly ("Authorized Users").

10. Queries made to the CTIC's data applications will be logged into the data system identifying the user initiating the query.

11. The CTIC will maintain an audit trail of inquiries, and accessed and disseminated CTIC data.

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

13. CTIC 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.

14. CTIC will immediately notify the originating agency from which CTIC received personal information of a suspected or confirmed breach of such information.

15. Users who are not employed by or assigned to CTIC, who are doing temporary work at CTIC, will be required to sign a nondisclosure agreement.

M. Information Retention and Destruction

1. All applicable information will be reviewed for record retention (validation or purge) by CTIC at least every five (5) years, as provided by 28 CFR Part 23. In addition see Connecticut General Statutes Section 11-8a, which describes state agency general responsibilities regarding records retention.

2. CTIC will identify information for destruction, purging and deletion in accordance with the CTIC retention and destruction policy established according to applicable law.

3. CTIC will remove, destroy or delete information once its retention period has expired as provided by this policy or as otherwise agreed upon with the originating agency in a participation or membership agreement.

4. CTIC will follow Connecticut state law, including Connecticut General Statutes §11-8a, and the regulations established thereunder, regarding retention and destruction of records unless pre-empted by federal law or court order.

5. No approval will be required from the originating agency before information held by CTIC is destroyed or returned in accordance with this policy or as otherwise agreed upon with the originating agency in a participation or membership agreement.

6. A record of information to be reviewed for retention will be maintained by CTIC and no notice will be given to the submitter prior to the required review and validation/purge date.

7. Notification of proposed destruction or return of records may or may not be provided to the originating agency by CTIC, depending on the relevance of the information and any agreement with the originating agency.

N. Accountability and Enforcement

1. Information System Transparency

A. CTIC's information and intelligence collection practices are contained within this Privacy Policy. The CTIC Privacy Policy will be provided to the public for review on the Department of Emergency Management and Homeland Security website at www.ct.gov/demhs.

B. The CTIC Privacy Officer will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections within CTIC's information systems. The Privacy Officer can be contacted at: CTIC Privacy Officer, Connecticut Department of Emergency Management and Homeland Security, 25 Sigourney Street, Hartford, CT 06106 or by e-mail at ctic.privacyofficer@ct.gov.

2. Accountability

A. The audit log of queries made to CTIC will identify the user initiating the query.

B. CTIC will maintain an audit trail of accessed, requested, or disseminated information. An audit trail will be kept for three years or longer as is required under the CTIC records retention policy or state law of requests for access to information for specific purposes and of what information is disseminated to each authorized user in response to the request.

C. CTIC will adopt and follow procedures and practices by which it can evaluate the compliance of users with system security and privacy. This includes at least annual system audits. A record of the audits will be maintained by the CTIC Security Officer.

D. CTIC's authorized users shall report errors and suspected or confirmed violations of CTIC policy relating to protected information to the CTIC Privacy Officer.

E. Each October, CTIC will conduct or arrange for an audit and inspection of the information contained in its information and intelligence systems and will prepare, or cause to be prepared, an audit report by December 15th. The audit will be conducted by an authorized designee or designees, and has the option of conducting a random audit, without announcement, at any time and without prior notice of the CTIC staff. This audit must protect the confidentiality, sensitivity, and privacy of the CTIC criminal intelligence system.

F. Each January, the CTIC Legal Working Group, in conjunction with the CTIC Privacy and Security Officers, will review and update the provisions protecting privacy, civil rights, and civil liberties contained in this policy. See Section C-2. Changes in applicable law, technology, the purpose and use of the information systems, and public expectations, may require updates to this CTIC Privacy Policy.

3. Enforcement

A. Consistent with the bylaws of the CTIC Executive Board, any applicable collective bargaining agreements, and any memorandum of agreement with a CTIC staff member's parent agency, if a complaint of noncompliance with this policy has been substantiated against a CTIC staff member, CTIC and/or his or her parent agency will take all appropriate actions against that staff member, including suspending or discontinuing access to information.

B. If a complaint of noncompliance with this policy is substantiated against a participating agency or other authorized user, CTIC and/or the parent agency will take all appropriate actions against the agency or user, consistent with the bylaws of the CTIC Executive Board, any applicable collective bargaining agreements, and any memorandum of agreement with a CTIC staff member's parent agency, including suspending or discontinuing access to information.

C. CTIC reserves the right to restrict the qualifications and number of personnel having access to CTIC information and to suspend or withhold service to any personnel violating the Privacy Policy. CTIC reserves the right to deny access to any participating agency user who fails to comply with the applicable restrictions and limitations of the CTIC Privacy Policy. CTIC reserves the right to suspend access-- of a CTIC staff member, participating agency or other authorized user-- to information pending the outcome of any investigation or review.

O. Training

1 CTIC will require the following individuals to participate in training programs regarding implementation of and adherence to the privacy, civil rights, and civil liberties policy:

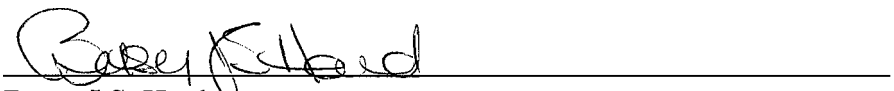
- All personnel assigned to CTIC;
- Personnel providing information technology services to CTIC; and,
- Staff assigned to CTIC from other public agencies or as private contractors providing services to CTIC.

2. CTIC will provide or arrange for training regarding the center's requirements and policies for collection, use, and disclosure of protected information to personnel

authorized to share protected information through the Information Sharing Environment.

3. The CTIC privacy policy training program will cover:

- Purposes of the privacy policy, including substance and intent;
- Civil rights, and civil liberties protections;
- Provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information;
- Recognition of originating and participating agency responsibilities and obligations under applicable law and policy;
- How to implement the policy in the day-to-day work of the user, whether a paper or systems user;
- The impact of improper activities associated with infractions within or through CTIC;
- Mechanisms for reporting violations of the CTIC Privacy Policy; and,
- Possible penalties for Privacy Policy violations.



Betsy J.S. Hard
Director, Connecticut Intelligence Center (CTIC)

12/6/10
Date

Appendix A
Terms and Definitions

The following is a list of primary terms and definitions used in this policy.

Agency: The Connecticut Intelligence Center (CTIC), under the Connecticut Department of Emergency Management and Homeland Security (DEMHS) and all agencies that access, contribute, and share information in the CTIC's justice information system.

Analysis: Development of a theory or broad concept of what occurred or may occur, who was involved or where and when it may happen in order to identify trends or alerts, warnings, notifications or information that will prevent a terrorist attack or criminal activity.

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

Audit trails are a fundamental part of computer security, used to trace (albeit usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

Center: Refers to the Connecticut Intelligence Center (CTIC).

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

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

Collation: Combining, sorting, and storage of information in order to enhance access and analysis.

Collection: Gathering raw data from all available sources needed to produce intelligence products and/or meet an intelligence requirement. Data may be collected from many sources, including but not limited to public records, the Internet, co dential sources, incident reports, and periodicals.

Criminal Intelligence Information: 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 activity. Criminal intelligence records are maintained in a criminal intelligence system pursuant to the requirements contained in 28 CFR Part 23.

CTIC: Connecticut Intelligence Center. CTIC is a regional intelligence center at which officials from a cross-section of law enforcement agencies work together to collect, store, analyze, share, and disseminate information on criminal and terrorist activities in an effort to counter such activities. CTIC also works to identify emerging terrorist threats or crime trends.

Cyber Security: The protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

Data Breach: The unintentional release of secure information to an untrusted environment. This may include incidents such as theft or loss of digital media—including computer tapes, hard drives, or laptop computers containing such media—upon which such information is stored unencrypted; storing information on a computer or data storage element having Internet connectivity without proper information security precautions; transfer of such information to a system that is not completely open but is not appropriately or formally accredited for security at the approved level, such as unencrypted e-mail; or transfer of such information to the information systems of a possibly hostile agency or environment where it may be exposed to more intensive decryption techniques.

Data Protection: Encompasses the range of legal, regulatory, physical and institutional mechanisms that guide the collection, use, protection, and disclosure of information.

Disclosure: The release, transfer, provision of access to, sharing, publication, or divulging of information in any manner—electronic, oral, or in writing—to an individual, agency, or organization outside the agency that collected it. Disclosure is an aspect of privacy, focusing on information which may be available only to certain people for certain purposes but which is not available to everyone.

Fair Information Principles: The Fair Information Principles (FIPs) is a framework of internationally recognized principles for protecting the privacy and security of personal information (GAO-08-543T). These principles 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,*** and allow for privacy interests to be balanced with policy related to such things as national security, law enforcement, and administrative efficiency. 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 OECD based FIPs are:

- **Collection Limitation:** The collection of personal information should be limited, should be obtained by lawful and fair means, and where appropriate, with knowledge or consent of the individual.
- **Data Quality:** Personal information should be relevant to the purpose for which it was collected, and should be accurate, complete, and current as needed for that purpose.
- **Purpose Specification:** The purposes for which personal data are collected should be disclosed before collection and upon any change to that purpose and its use should be limited to those purposes and compatible purposes.
- **Use Limitation:** Personal information should not be disclosed or otherwise used for other than a specified purpose without consent of the individual or legal authority.
- **Security Safeguards:** Personal information should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.
- **Openness:** The public should be informed about privacy policies and practices, and individuals should have ready means of learning about the use of personal information.
- **Individual Participation:** Individuals should have the rights to: know about the collection or use of personal information, to access that information, to request correction, and to challenge the denial of those rights.

- **Accountability:** Individuals controlling the collection or the use of personal information should be accountable for taking steps to ensure the implementation of these principles.

Fusion Center: A collaborative effort of two or more agencies that provide resources, expertise, and/or information to a designated government agency or agency component with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal activity. The primary components of a fusion center are situational awareness and warnings that are supported by law enforcement intelligence, derived from the application of the intelligence process, where requirements for actionable information are generated and information is collected, integrated, evaluated, analyzed, and disseminated. Other key components resident in the fusion center include representatives of public safety, homeland security, the private sector, and critical infrastructure communities. (DOJ, DHS Fusion Center Guidelines, p.12)

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.

Information: Includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists. Information received by law enforcement agencies can be categorized into four general areas: general data; tips and leads data; suspicious activity reports; and criminal intelligence information.

Information Quality: Refers to various aspects of the information; the accuracy and validity of the actual values of the data, data structure, and database/data repository design. Traditionally, the basic elements of information quality have been identified as accuracy, completeness, currency, reliability, and context/meaning. Today, information quality is being more fully described in multidimensional models, expanding conventional views of the topic to include considerations of accessibility, security, and privacy.

Information Sharing Environment (ISE) Suspicious Activity Report (SAR) (ISE-SAR): A suspicious activity report that has been determined to have a potential terrorism nexus. ISE-SAR business rules will serve as a unifying process to support the reporting, tracking, processing, storage, and retrieval of terrorism-related suspicious activity reports across the ISE.

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 the United States of America 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: A necessary part of an adequate security system to ensure that data is properly tracked and that only authorized individuals are getting access to the system and the data. See also Audit Trail.

Need to Know: A determination made by an authorized holder of information that a prospective recipient requires access to the information in order to perform or assist in a lawful and authorized governmental function.

Originating Agency: The agency or organizational entity that documents information or data, including source agencies that document SAR (and, when authorized, ISE-SAR) information that is collected by a fusion center: the owner of data.

Participating Agencies: An organizational entity that is authorized to access or receive and use CTIC information and/or intelligence databases and resources for lawful purposes through its authorized individual users: may include source agencies and submitting agencies.

Personal Information: Information that can be used, either alone or in combination with other information, to identify individual subjects suspected of engaging in criminal activity, including terrorism.

Personally Identifiable Information: Any information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to an individual. Personally identifiable information may include personal characteristics, or a unique set of numbers or characters associated with a specific individual (including name, address, zip code, phone number, social security number, email address, driver's license number, financial account or credit card number and associated PIN number, Integrated Automated Fingerprint Identification System [IAFIS], or booking or detention

system number. It may also include a description of events or a moment in time (e.g., police report) or a description of a location or place (e.g., GIS location.)

Privacy: An individual's 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.

Privacy Policy: A written, published statement that articulates the policy position of an organization on how it handles the personal information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, disseminatioddisclosure, and access. A well-developed and implemented privacy policy uses justice entity resources wisely and effectively; protects the organization, the individual, and the public; and promotes public trust.

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

Protected Information: Protected information includes personally identifiable information that is subject to information privacy or other legal protections by law, including the U.S. Constitution and the Connecticut Constitution; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 23; and applicable state statutes and regulations. Protection may also be extended to organizations by CTIC policy or state law.

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 center'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 center or participating agency.

Public does not include:

- Employees of CTIC or participating agency;
- People or entities, private or governmental, who assist CTIC in the operation of the justice information system;

- Public agencies whose authority to access information gathered and retained by CTIC is specified in law.

Redress: Laws, policies, and procedures that address public agency responsibilities with regard to access/disclosure and correction of information and the handling of complaints from persons regarding protected information about them which is under an organization's (including a fusion center's) control and which is exempt from disclosure and not disclosed to the individual to whom the information pertains.

Retention: Refer to Storage.

Right to Know: Based on having legal authority or responsibility or pursuant to an authorized agreement, an agency or organization is authorized to access sensitive information and intelligence in the performance of a law enforcement, homeland security, or counterterrorism activity. May also mean that an individual requesting access to criminal intelligence data has the right to access due to legal authority to obtain the information pursuant to a court order, statute or decisional law."

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

Security: Refers to the range of administrative, technical, and physical business practices and mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes. Computer and communications security efforts also have the goal of ensuring the accuracy and timely availability of data for the legitimate user set, as well as promoting failure resistance in the electronic systems overall. May also refer to a series of procedures and measures which, when combined, provide protection of people from harm; information from improper disclosure or alteration; and, assets from theft or damage.

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

Standing Intelligence Needs (SINs): Prioritized Information needs that serve as a guide for intelligence collection efforts and reporting activities in Connecticut.

Storage: In a computer, storage is the place where data is held in an electromagnetic or optical form for access by a computer processor.

With regard to the ISE, storage (or retention) refers to the storage and safeguarding of terrorism-related information—including homeland security information, terrorism information, and law enforcement information relating to terrorism or the security of the

United States of America or any part thereof, --by both the originator of the information and any recipient of the information.

Suspicious Activity: Defined in the ISE-SAR Functional Standard (Version 1.5) as "observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity." Examples of suspicious activity include, but are not limited to, surveillance, photography of potentially sensitive infrastructure facilities, site breach or physical intrusion, cyber attacks, testing of security.

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

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

Terrorism-Related Information: In accordance with the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended by the 9/11 Commission Act (August 3,2007, P.L. 110-53), the ISE facilitates the sharing of terrorism and homeland security information, as defined in IRTPA Section 1016(a)(5) and the Homeland Security Act 892(f)(1) (6 U.S.C. § 482(f)(1)). See also ***Information Sharing Environment Implementation Plan*** (November 2006) and Presidential Guidelines 2 and 3 (the ISE will facilitate the sharing of "terrorism information," as defined in the IRTPA, as well as the following categories of information to the extent that they do not otherwise constitute "terrorism information": (1) homeland security information as defined in Section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. § 482(f)(1)); and (2) law enforcement information relating to terrorism or the security of our homeland). Such additional information may include intelligence information. P.L. 110-53 amends the definition of terrorism information to include information regarding weapons of mass destruction.

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

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

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

APPENDIX B
Connecticut Statutory Provisions with an Impact on the Disclosure of Records[1]

C.G.S. Sec. 1-17a Prohibitions on disclosure of photographs and computerized images of individuals.

C.G.S. Sec. 1-210 FOIA Exemptions

C.G.S. Sec. 1-211 Disclosure of electronically stored records

C.G.S. Sec. 1-215 Records of arrest

C.G.S. Sec. 1-216 Uncorroborated allegations of criminal activity

C.G.S. Sec. 1-217 Nondisclosure of residential addresses of individuals holding designated positions

C.G.S. Sec. 4b-131(b) Nondisclosure of security records

C.G.S. Sec. 8-360 Confidentiality of location of housing for domestic violence victim

C.G.S. Sec. 14-10 Disclosure of personal information and highly restricted personal information contained in motor vehicle records.

C.G.S. Sec. 17a-28(i) name of individual reporting child abuse/neglect

C.G.S. Sec. 17a-28(j) name of individual cooperating with abuse/neglect investigation confidential

C.G.S. Sec. 17a-101k information relative to child abuse confidential

C.G.S. Sec. 19a-411 Autopsy Reports

C.G.S. Sec. 29-10c Accident Records

C.G.S. Sec. 29-11 SPBI records

C.G.S. Sec. 29-16 Use of SPBI information

---

[1] It should be noted that certain records may be subject to seal or non-disclosure by court order, settlement agreement or pursuant to a provision of federal law.

C.G.S. Sec. 29-28(d) Name and address of individual holding permit to sell or permit to carry a pistol or revolver protected fiom disclosure

C.G.S. Sec. 29-36g Name and address of individual holding eligibility certificate protected fiom disclosure

C.G.S. Sec. 29-164f National Crime Prevention and Privacy Compact

C.G.S. Sec. 29-171 Illegal disclosure of SOCITF information or name of informant

C.G.S. Sec. 42-470 Social Security Numbers

C.G.S. Sec. 46b-124 Co dentiality of records of juvenile matters

C.G.S. Sec. 46b-133a. Erasure of delinquency records

C.G.S. Sec. 46b-146 Erasure of police and court records regarding delinquent child or a member of a family with service needs

C.G.S. Sec. 46b-133a Erasure of records upon nolle prosequi of delinquency charge

C.G.S. Sec. 51-5c (b) (1) Confidentiality of information in registry of protective orders

C.G.S. Sec. 53-202(g) Machine registration data not subject to public inspection

C.G.S. Sec. 53-202d Name and address of individual holding certificate of possession of assault weapon protected fiom disclosure

C.G.S. Sec. 54-41p Unauthorized disclosure of contents of wire communication

C.G.S. Sec. 54-76l Records of youthful offender confidential

nfi

C.G.S. Sec. 54-76o Erasure of police records and court records of youthful offender

C.G.S. Sec. 54-86e Confidentiality of name and address of victim of sexual assault

C.G.S. Sec. 54-142a Erased criminal records

C.G.S. Sec. 54-142c Disclosure of erased records

Chapter 961a, Part II Security and Privacy of Criminal Records

Appendix C
Federal Laws Relevant to Seeking, Retaining, and Disseminating Justice Information

***Excerpt** from*
U.S. Department of Justice's** (DOJ's) **Privacy, Civil Rights, and Civil Liberties Policy Templates for Justice Information Systems

The U.S. Constitution is known as the primary authority that applies to federal as well as state, local, and tribal (SLT) agencies. State constitutions cannot provide fewer privacy and other civil liberties protections than the U.S. Constitution but can (and many do) provide enhanced privacy and other civil liberties protections.

Civil liberties protections are primarily founded in the Bill of Rights. They include the basic freedoms, such as free speech, assembly, and religion; freedom from unreasonable search and seizure; due process; etc. The relationship of these fundamental rights to the protection of privacy, civil rights, and other civil liberties in the Information Sharing Environment is explored in a key issues guidance paper titled ***Civil Rights and Civil Liberties Protection,*** which is available on the Program Manager (PM) for the Information Sharing Environment (PM-ISE) Web site at www.ise.gov.

Statutory civil rights protections in the U.S. Constitution may, in addition, directly govern state action. These include the Civil Rights Act of 1964, as amended; the Rehabilitation Act of 1973; the Equal Educational Opportunities Act of 1974; the Americans with Disabilities Act; the Fair Housing Act; the Voting Rights Act of 1965; and the Civil Rights of Institutionalized Persons Act.

Federal laws, Executive Orders, regulations, and policies directly affect agencies'/centers' privacy policies. While SLT agencies may not be generally bound directly by most statutory federal privacy and other civil liberties protection laws in the information collection sharing context, compliance may be required **indirectly** by funding conditions (e.g., 28 CFR Parts 20, 22, and 23 or the Health Insurance Portability and Accountability Act [HIPAA]); operation of the Commerce Clause of the U.S. Constitution (e.g., Electronic Communications Privacy Act of 1986); or a binding agreement between a federal agency and an SLT agency (e.g., a memorandum of agreement or memorandum of understanding). Where relevant or possibly relevant, agencies/centers are advised to list these laws, regulations, and policies, noting those

that may potentially affect the sharing of information, including sharing terrorism-related information in the Information Sharing Environment.

The development of a privacy, civil rights, and civil liberties policy is primarily designed for center personnel and authorized users to ensure that they are aware of the legal and privacy framework within which they and the center must operate. If the applicability and requirements of various laws, regulations, or sharing agreements are not spelled out or referenced in an center privacy policy, staff and user accountability is greatly diminished, mistakes are made, privacy violations occur, and the public's (and other agencies') confidence in the ability of the center to protect information and intelligence is compromised. When staff members know the rules through sound policy and procedure communicated through ongoing training activity, information sharing is enhanced.

Following is a partial listing of federal laws that should be reviewed when developing a privacy policy for a justice information system. The list is arranged in alphabetical order by popular name.

Brady Handgun Violence Prevention Act, 18 U.S.C. §§ 921, 922, 924, and 925A, United States Code, Title 18, Part I, Chapter 44, §§ 921,922,924, and 925A

Computer Matching and Privacy Act of 1988, 5 U.S.C. § 552a(a), United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a(a); see also Office of Management and Budget, Memorandum M-01-05, "Guidance on Interagency Sharing of Personal Data–Protecting Personal Privacy," December 20,2000

Confidentiality of Identifiable Research and Statistical Information, 28 CFR Part 22, Code of Federal Regulations, Title 28, Chapter I, Part 22

Crime Identification Technology, 42 U.S.C. § 14601, United States Code, Title 42, Chapter 140, Subchapter I, $14601

Criminal History Records Exchanged for Noncriminal Justice Purposes, 42 U.S.C. § 14611, United States Code, Title 42, Chapter 140, Subchapter II, § 14611

Criminal Intelligence Systems Operating Policies, 28 CFR Part 23, Code of Federal Regulations, Title 28, Chapter 1, Part 23

Criminal Justice Information Systems, 28 CFR Part 20, Code of Federal Regulations, Title 28, Chapter 1, Part 20

Disposal of Consumer Report Information and Records, 16 CFR Part 682, Code of Federal Regulations, Title 16, Chapter I, Part 682

Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2522, 2701–2709, United States Code, Title 18, Part I, Chapter 119, §§ 2510–2522, 2701–2709, and 3121–3125, Public Law 99-508

Fair Credit Reporting Act, 15 U.S.C. § 1681, United States Code, Title 15, Chapter 41, Subchapter III, § 1681

Federal Civil Rights laws, 42 U.S.C. § 1983, United States Code, Title 42, Chapter 21, Subchapter, § 1983

Federal Records Act, 44 U.S.C. § 3301, United States Code, Title 44, Chapter 33, § 3301

Freedom of Information Act (FOIA), 5 U.S.C. § 552, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552

HIPAA, Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 201, United States Code, Title 42, Chapter 6A, Subchapter I, § 201; Public Law 104-191

HIPAA, Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164; Code of Federal Regulations, Title 45, Parts 160 and 164

Indian Civil Rights Act of 1968, 25 U.S.C. § 1301, United States Code, Title 25, Chapter 15, Subchapter I, § 1301

Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Section 1016, as amended by the 9/11 Commission Act

National Child Protection Act of 1993, Public Law 103-209 (December 20, 1993), 107 Stat. 2490

National Crime Prevention and Privacy Compact, 42 U.S.C. § 14616, United States Code, Title 42, Chapter 140, Subchapter II, § 14616

Privacy Act of 1974, 5 U.S.C. § 552a, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a

Privacy of Consumer Financial Information, 16 CFR Part 313, Code of Federal Regulations, Title 16, Chapter I, Part 313

Protection of Human Subjects, 28 CFR Part 46, Code of Federal Regulations, Title 28, Chapter 1, Volume 2, Part 46

Safeguarding Customer Information, 16 CFR Part 314, Code of Federal Regulations, Title 16, Chapter I, Part 314

Sarbanes-Oxley Act of 2002, 15 U.S.C., Chapter 98, § 7201, United States Code, Title 15, Chapter 98, § 7201

U.S. Constitution, First, Fourth, and Sixth Amendments

USA PATRIOT Act, Public Law 107-56 (October 26, 2001), 115 Stat. 272