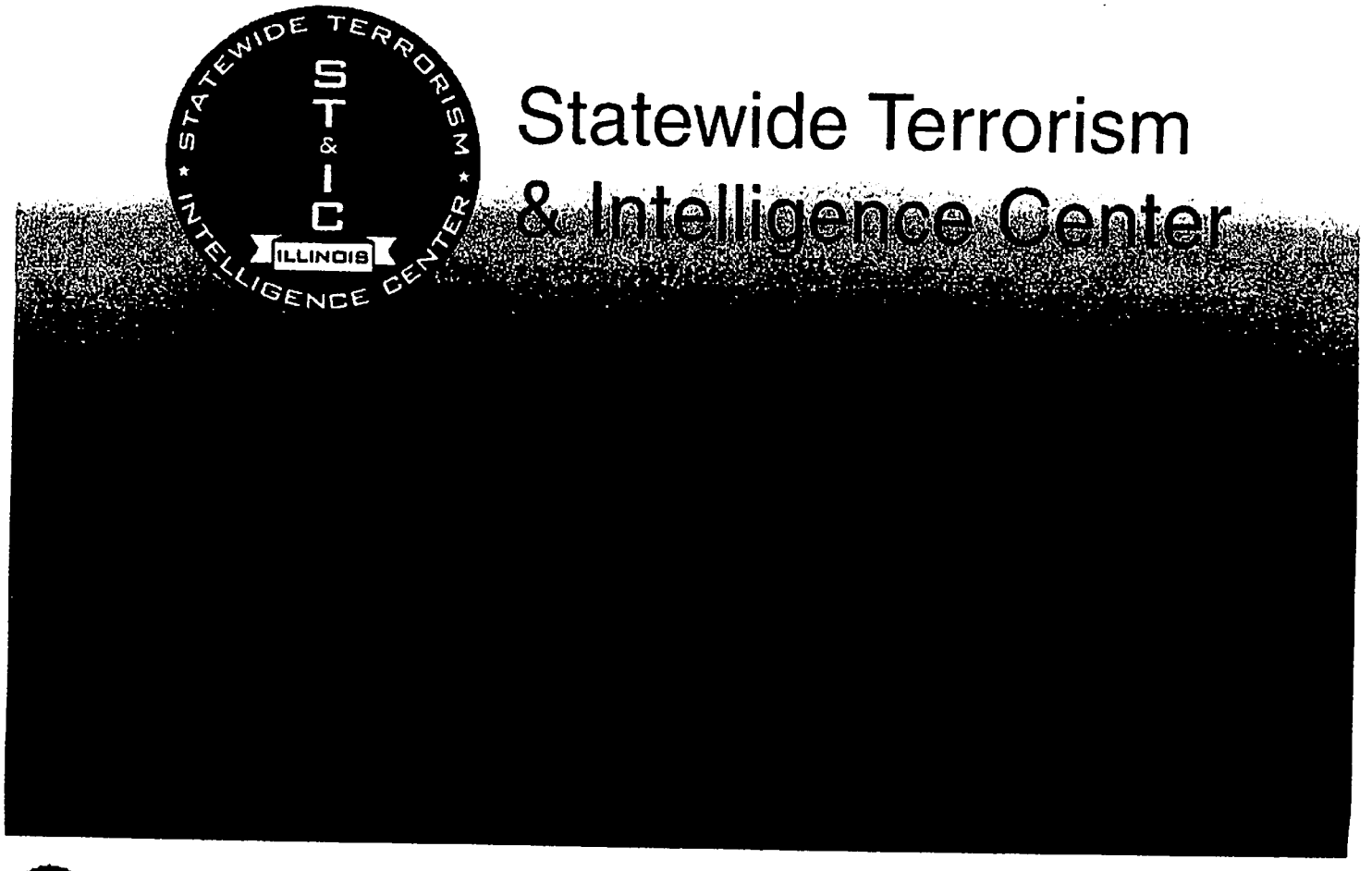
STIC Privacy Policy



Illinois State Police

Illinois State Police
Statewide Terrorism & Intelligence Center
Privacy Policy

April 2010

Article I. Mission Statement

The mission of the Illinois State Police (ISP) Statewide Terrorism & Intelligence Center (STIC) is to collect, evaluate, analyze, and disseminate information and intelligence data regarding criminal, terrorist and all-hazards[1] activities.[2] The STIC is comprised of intelligence and public safety officials from federal, state, and local law enforcement agencies whose primary goal is to provide timely, accurate, and actionable intelligence to public safety and private-sector partners. STIC operations enhance public safety, facilitate communication between agencies, and provide support in the fight against terrorism and criminal activity.

This Privacy Policy applies to all individuals unless otherwise specified. It describes how personally identifiable information is collected, used and secured. This Policy was prepared by the ISP Privacy Office and is designed to protect the privacy rights of U.S. citizens and other specified individuals.

Article II. Compliance and Governance

All intelligence personnel, participating agency personnel, private contractors, and other authorized individuals[3] are required to abide by this Privacy Policy and applicable laws which govern the treatment of the information the center collects, receives, maintains, archives, accesses, or discloses. All intelligence personnel are required to provide written acknowledgement of receipt of this Privacy Policy and written agreement with its compliance. Nothing in this policy is intended to create a private right of action for any member of the public or alter existing or future federal and state law requirements.

STIC has adopted standard operating procedures and policies that comply with federal and Illinois law[4] concerning the appropriate collection, analysis, dissemination and retention of personally identifiable information and intelligence data.

The Illinois State Police Director has the primary responsibility for the overall operation of STIC including, but not limited to, its information systems, personnel, and operations.

Reports regarding alleged violations and suggestions for amendments shall be submitted to the Illinois State Police Privacy Office.[5]

---

[1] "All-hazards" is defined as events or incidents including, but not limited to, major accidents, natural disasters, and terrorist-related activity.
[2] 20 ILCS 2605/2605-45(4).
[3] Hereinafter referred to as "intelligence personnel."
[4] 28 Code of Federal Regulations (CFR) Part 23; 20 ILCS 2605/2605-45(4).
[5] These reports will be retained subject to the Illinois State Records Act, 5 ILCS 160.

Article III. Definitions

(1) **Actionable intelligence** - a relatively small piece or pieces of non-obvious detail(s) that can form an initial basis point for hypothesis building.

(2) **Authorized persons** - Terrorism Research Specialists, Criminal Intelligence Analysts, Critical Infrastructure Specialists, Watch Officers, field intelligence personnel, public safety officials, certified police officers, and other criminal justice administrative and intelligence personnel in the furtherance of their official duties.

(3) **Authorized users** - Terrorism Research Specialists, Criminal Intelligence Analysts, Critical Infrastructure Specialists, Watch Officers, field intelligence personnel, public safety officials, certified police officers, and other criminal justice administrative and intelligence personnel who meet certain qualifications outlined in this Policy.

(4) **Individuals** - encompasses individuals as well as any group, association, corporation, business, partnership or other organization.

(5) **Personally identifiable information** - any data that can be used to uniquely identify, contact, or locate a single person or entity.

(6) **Private right of action** - a term used in United States statutory and constitutional law for circumstances a court will determine that a law that creates rights also allows private parties to bring a lawsuit, even where no such remedy is expressly provided for in the law.

(7) **Public Safety Official** - a public safety official, serving with or without compensation, working in a public agency in an official capacity, including but not limited to a law enforcement officer, intelligence analyst, firefighter, or member of emergency medical response organization

(8) **U.S. Citizen** - individuals born in the United States, Puerto Rico, Guam, Northern Mariana Islands, Virgin Islands, American Samoa, or Swain's Island; foreign-born children, under age 18, residing in the U.S. with their birth or adoptive parents, at least one of whom is a U.S. citizen by birth or naturalization; or individuals granted citizenship status by Immigration and Naturalization Services.

(9) **VITAL** - Violent Crime Information Tracking and Linking System is ISP's data system that stores criminal justice data collected by intelligence personnel.

Article IV. STIC Overview

A. Intelligence Personnel

(1) All STIC and field intelligence personnel (hereinafter referred to as intelligence personnel) are subject to the provisions of this Privacy Policy.

(2) Intelligence personnel include:

- (a) **Terrorism Research Specialists** who research and analyze potential terrorism suspect and incident data;
- (b) **Criminal Intelligence Analysts** who research and analyze potential criminal activity, suspect, and incident data;
- (c) **Critical Infrastructure Specialists** who research and analyze potential threats to critical infrastructure; and
- (d) **Supervisors**
  - (i) **Watch Officer** – First level of supervision within STIC; oversees the day-to-day supervision, decision-making, and quality control functions.
  - (ii) **Assistant Center Chief (ACC)** – Provides administrative and supervisory oversight to the Watch Officers.
  - (iii) **Center Chief (CC)** – Responsible for all functions and activities of STIC and its employees; provides administrative and supervisory oversight to the ACC.

B. Division of Administration (DOA) Personnel

(1) Select ISP DOA personnel have access to information contained in law enforcement data systems and criminal intelligence data stores for the limited purpose of providing technical assistance.

(2) DOA personnel who have access to intelligence data are subject to the provisions of this Privacy Policy.

(3) Notwithstanding any provisions of this policy to the contrary, DOA personnel shall not disseminate criminal intelligence information.

C. STIC Data Sources

(1) Intelligence personnel gather information from a variety of data sources. Specifically, personnel access information contained in law enforcement data systems, criminal intelligence data stores, and publicly available records. Depending upon the type of investigation or potential criminal conduct, Intelligence personnel query certain specified data sources and compile information about individuals or groups for appropriate dissemination in accordance with this Policy.

- (a) **Law Enforcement Data Systems** – Intelligence personnel may access traditional sources of law enforcement data.
- (b) **Criminal Intelligence Data Stores** – Intelligence personnel have access to intelligence information submitted by law enforcement agencies and maintained internally.
- (c) **Publicly Available Records** - Intelligence personnel may access public records through various public and privately compiled sources.

Article V. General Operating Procedures

The U.S. Department of Justice has promulgated administrative rules at 28 Code of Federal Regulations (CFR) Part 23. These regulations were designed to bring about an equitable balance between the civil rights and liberties of citizens and the needs of law enforcement to collect and disseminate criminal intelligence on the conduct of identifiable persons and groups who may be engaged in systematic criminal activity. The following procedures are intended to implement these regulations and apply to STIC operations and personnel absent a more stringent provision adopted herein.

A. Criminal Intelligence File

(1) A criminal intelligence file consists of stored information on the activities and associations of:
   (a) Individuals who are reasonably suspected of being involved in the actual or attempted planning, organizing, financing, or commission of criminal acts; or
   (b) Individuals who are reasonably suspected of being involved in criminal activities with known or suspected crime figures; or
   (c) Organizations, businesses, and groups that are reasonably suspected of being substantially and significantly involved in the actual or attempted planning, organizing, financing, or commission of criminal acts (criminal organizations); or
   (d) Organizations, businesses, and groups that are reasonably suspected of being operated, controlled, financed, or infiltrated by known or suspected crime figures for use in an illegal manner.

(2) Types of Crimes Resulting in the Creation of an Intelligence File
   (a) Any suspected crime that, in the reasonable judgment of the submitting agency or officer, represents a significant and recognized threat to the population and: (1) poses a threat to the life or property of citizens; (2) involves a permanent criminal organization; or (3) is not limited to one jurisdiction.

B. Standards for Initiating a Query

(1) Intelligence personnel may provide to law enforcement officials, upon request, criminal intelligence information upon a showing of reasonable suspicion of a crime.[6]

C. Collection Standards/Record Entry

(1) Intelligence personnel may collect and maintain criminal intelligence information concerning an individual or a group reasonably suspected of criminal conduct or activity.

(2) Intelligence personnel will collect and maintain a record of the source of the information.[7]

(3) For purposes of this Policy, reasonable suspicion 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.

(4) Intelligence personnel are responsible for establishing the existence of reasonable suspicion of criminal activity prior to submitting information about an individual or group into any intelligence data system.

(5) Information submitted to an intelligence system must be relevant to the suspected criminal activity and subject identification.

(6) Criminal intelligence information that intelligence personnel submit to an intelligence system shall be labeled to indicate the level of sensitivity of the record and the level of confidence in the information in accordance with this Policy.

(7) STIC systems may include non-criminal identifying information in a criminal intelligence information submission, provided sufficient precautions are in place to make it clear to users the two different types of data that are being accessed.[8]

(8) The ISP retains the right to reject any data element that is not relevant or that could pose an unreasonable risk of harm to the public.

(9) Investigative techniques employed by Intelligence personnel shall be lawful and only so intrusive as to gather sufficient information to prevent criminal conduct or the planning of criminal conduct.

(10) Intelligence personnel may not collect and maintain information concerning race, ethnicity, citizenship, place of origin, age, disability, gender, sexual orientation, political, religious, or social views,

---

[6] The reasonable suspicion requirement represents a higher standard than required by 28 CFR Part 23.20(e); Queries will not be conducted based solely upon violation of traffic laws.

[7] The record of the source of the information shall contain, where relevant and appropriate: (1) the name of the originating department, component, and subcomponent; (2) the name of the agency system from which the information is disseminated; (3) the date the information was collected and the date its accuracy was last verified; and (4) the title and contact information for the person to whom questions regarding the information should be directed.

[8] The 1998 Policy Clarification to 28 CFR Part 23.

associations, or activities of any individual or any group unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in such criminal conduct or activity.

D. Data Quality

(1) Prior to entering information into any intelligence system, intelligence personnel shall evaluate the reliability of each data source and assess the content validity of the data. Proper labels shall be applied to all data submitted to an intelligence system.

(2) If intelligence personnel have cause to believe the data contains an error or deficiency, they must contact the VITAL Quality Control Crime Information Evaluator for coordination with the source of the data.

(3) Random VITAL audits are performed on a continual basis by VITAL Quality Control.

(4) Intelligence personnel shall use the following labels for source reliability:
   (a) Highly Reliable - The reliability of the source is unquestioned or has been well tested in the past.
   (b) Usually Reliable - The reliability of the source can usually be relied upon as factual. The majority of information provided in the past has proven to be reliable.
   (c) Not Often Reliable - The reliability of the source has been sporadic in the past.
   (d) Unknown -The reliability of the source cannot be judged. Its authenticity or trustworthiness has not yet been determined by either experience or investigation.

(5) ISP VITAL maintains a record of the source of the information.[9]

(6) Intelligence personnel shall use the following labels for content validity:
   (a) Factual - The information has been corroborated by an investigator or another independent, reliable source.
   (b) Possibly True - The information is consistent with past accounts.
   (c) Hearsay - The information is inconsistent with past accounts.
   (d) Unknown - The authenticity of the information has not yet been determined by either experience or investigation.

(7) A data element with a source reliability of "Unknown" and a validity assessment of "Unknown" may not be entered into an intelligence system.

(8) Intelligence personnel will respond to any requests from authorized users for validation of previously disseminated data and, when information is identified that may be inaccurate or incomplete, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the rights of an individual may be

[9] *Supra* note 8.

affected, provide notice to authorized users who are known to have received the information.[10]

E. Classifications

(1) Prior to entering information into any intelligence system, intelligence personnel shall classify the data in order to protect sources, investigations, and the data subject's right to privacy. Intelligence personnel will treat information pertaining to any individual with the exact same level of privacy protection. Classification also indicates whether internal approval must be completed prior to the release of the information to persons outside STIC.

(2) STIC classifies data into the following categories:

(a) **Confidential** – Confidential information is the highest level of unclassified but sensitive information. Access to information defined as "confidential" is limited, even among law enforcement officers.

(b) **Law Enforcement Sensitive (LES)** – LES information is middle level unclassified but sensitive information. LES may be disseminated to law enforcement personnel only.

(c) **For Official Use Only (FOUO)** – FOUO is unclassified information of a sensitive nature which can be disseminated outside the scope of law enforcement personnel (i.e., participating agency personnel, private contractors, and other authorized individuals). FOUO may not be released to the general public.

(d) **Protected Critical Infrastructure Information (PCII)** – Protected Critical Infrastructure Information (PCII) is a subset of Critical Infrastructure Information for which protection is requested under the PCII Program by the requestor. Critical Infrastructure Information is information related to the security of critical infrastructure or protected systems that are not customarily in the public domain.

(e) **Open Source** – Open source information is any information that is publicly available. This information will be marked as "Unclassified" using an indicator of (U).

(3) **Classification** - All intelligence information has its security classification marked directly on the information file.

(4) **Re-evaluation of Classification**
Re-evaluations can be based upon time (i.e., tied to the five-year retention/renewal); the addition of new information; or at the time of a request for the information.

[10] As required by 28 CFR Part 23.20(h).

F. Labeling

(1) All criminal intelligence information disseminated will be labeled as such so that the recipient can handle the information in accordance with applicable legal requirements.
(2) Information labeled as non-intelligence information will be maintained and disseminated in the same manner as intelligence information.
(3) The data contained within STIC criminal intelligence systems will be identified as intelligence or non-intelligence information and any applicable legal requirements for handling such data indicated is provided in paragraph E of this Article.

G. Dissemination

(1) Intelligence personnel may disseminate criminal intelligence information only to law enforcement or criminal investigative authorities who agree to follow procedures regarding the receipt, maintenance, security, and dissemination of information that are consistent with 28 CFR Part 23 and this Policy.
(2) Intelligence personnel may disseminate criminal intelligence information to law enforcement or criminal investigative authorities who demonstrate a need and right to know the information in the performance of a law enforcement activity.[11]
(3) Intelligence personnel may disseminate an assessment (not including personally identifiable information) of criminal intelligence information to any individual where necessary to avoid imminent danger to life or property.
(4) An access log/audit trail or dissemination record is required when the database is accessed or information is disseminated from the intelligence system. This record can be created automatically by the database, or policies and procedures can be implemented to handle the access log/audit trail or dissemination record manually. The dissemination record shall contain the following information:
    (a) The date of dissemination of the information;
    (b) The name of the individual requesting the information;
    (c) The name of the agency requesting the information;
    (d) The reason for the release of the information (i.e., a description of the need to know and right to know);
    (e) The information provided to the requester; and
    (f) The name of the individual from STIC disseminating the information.
(5) Secondary dissemination of STIC data is permissible provided the dissemination would have been allowable directly from STIC systems under the terms of this Policy.

[11] Need to know is established where the prospective recipient requires access to specific information in order to perform or assist in a lawful and authorized governmental function (i.e., access is required for the performance of official duties). Right to know is established where the prospective recipient is an authorized individual acting in furtherance of a valid law enforcement or public safety function.

H. Review and Purge Procedures[12]

(1) Intelligence personnel will make every reasonable effort to ensure that information maintained in intelligence systems about individuals is current, accurate, and relevant. To accomplish this, intelligence personnel shall annually review intelligence information. The maximum retention period is five years, unless the intelligence information is validated and updated to ensure continuing compliance with system submission criteria.

(2) STIC intelligence databases automatically run daily checks for data that has met the five-year retention period. Data that has not been validated is purged.

(3) The entire record including all accompanying descriptive, identifying, and non-criminal identifying data must be validated. A record must be maintained of the name of the reviewer, date, and explanation of why the information is retained. Once validated, the retention period for the information may be extended for up to five more years.

(4) If the information has not been updated and/or validated, it must be removed from the system at the end of the retention period. Material purged from the intelligence system shall be destroyed.[13]

(5) Information removal must be approved by STIC Chief or designee.

(6) STIC will retain a record of dates when information is to be removed (purged) if not validated prior to the end of its five-year period.

(7) Non-intelligence information will be maintained and/or destroyed in accordance with the Illinois State Records Act.[14]

I. Security Procedures

(1) STIC is committed to protecting privacy and maintaining the integrity and security of personal information. STIC shall be responsible for implementing the following security requirements for its intelligence systems.

(2) STIC has formally adopted the Criminal Justice Information Systems (CJIS) Security Policy of the U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division[15] and applies these provisions to STIC operations. STIC will develop a separate security policy.

(3) Firewalls are in place to prevent unauthorized agencies or entities from accessing STIC resources.

(4) **Role-based user access** – The intelligence systems that intelligence personnel access utilize various levels of role-based user access.

(a) Each user's role shall determine the types of information accessible to the user.

---

[12] 28 CFR Part 23; 20 ILCS 2605/2605-45(4).
[13] Electronic records are permanently deleted and paper files are shredded.
[14] 5 ILCS 160/.
[15] May 2006 Version 4.3.

(b) Each user's role contains certain permissions to modify or delete records.

(5) **Security breaches and security breach notification** –ISP will monitor and respond to security breaches or breach attempts.[16]

(a) In the event that intelligence personnel become aware of a breach of the security of unencrypted personal information, ISP will notify an individual about whom personal information was or is reasonably believed to have been obtained by an unauthorized person and access to which threatens the physical or financial harm to the person.

(b) Any necessary 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.

(6) **Physical Safeguards** – STIC systems shall be located in a physically secured area that is restricted to designated authorized personnel.

(a) Only designated authorized personnel will have access to information stored in the STIC data systems.

(b) All authorized visitors, regardless of agency, are required to register with designated authorized personnel prior to gaining admission to the facility.

(c) All authorized registered visitors will be escorted by designated authorized personnel for the duration of the visit.

(7) **Disaster Recovery** – ISP has appropriate disaster recovery procedures for STIC data outlined in ISP's Disaster Recovery Plan.

(8) **Information Security Officers** - Federal agencies housed at STIC each have a dedicated information security officer. STIC has an Information Security Officer who is trained and handles network access/security.

(9) **Assessment Storage** - Risk and vulnerability assessments are stored separately from law enforcement and intelligence data. Risk and vulnerability assessments are not available to the public.

J. Training

(1) **Personnel Training**

(a) STIC has adopted the Department of Homeland Security Standards as the education and training standard for its Terrorism Research Specialists, Criminal Intelligence Analysts, and Critical Infrastructure Specialists.

(b) All intelligence personnel are provided training on this Privacy Policy.

---

[16] *See* 815 ILCS 530/.

(c) DOA personnel who have access to STIC data are provided training on this Privacy Policy.
(d) Training is provided on this Privacy Policy to all intelligence personnel, including Watch Officers, Statewide Zone Intelligence Officer Coordinator and Management (Center Chief and Assistant Center Chief).
(e) STIC will provide training to personnel authorized to access and/or disseminate data, including terrorism-related data.
(f) The ISP Privacy Officer is a licensed attorney and a Certified Information Privacy Professional.
(g) Private sector personnel in contractual relationships with ISP STIC will receive training on this Privacy Policy.

(2) **Policy Awareness**
(a) This Privacy Policy will be displayed for general view on the ISP website.
(b) Individuals authorized to access or disseminate intelligence information from STIC will be provided access to and acknowledge a thorough understanding of this Privacy Policy.

(3) **Policy Updates**
(a) The ISP Privacy Officer will update this Privacy Policy as new information sources are accessed through STIC.
(b) The ISP Privacy Officer will monitor legislative activity and update this Privacy Policy accordingly.
(c) The ISP Privacy Office will review this Privacy Policy annually and update it accordingly.
(d) Updated policies will contain the policy revision date and version number.
(e) Individuals authorized to access or disseminate intelligence information from STIC will be informed of policy updates as they become effective.

Article VI. STIC Data Sources

A. Law Enforcement Data Sources

Data from the following systems is not aggregated into a central database or repository. Rather, an analyst accesses each system separately to acquire relevant records related to a data subject. This list is not static but may change in the future as databases are merged, new databases are added or databases that do not prove useful to the mission of STIC are removed.

(1) The Illinois Law Enforcement Agencies Data System (LEADS) is a statewide, computerized, telecommunications system, maintained by the Illinois State Police, designed to provide the Illinois criminal justice community with access to computerized justice-related information from both the state and national level. Data within LEADS includes, but is not limited to, active warrants, federal criminal information and files from the Illinois Secretary of State (SOS).

(2) Citizen and Law Enforcement Analysis and Reporting system (CLEAR) is an information technology system managed by the Chicago Police Department enabling Chicago police to quickly share police incident report data and crime mapping software, among other types of information.

(3) El Paso Intelligence Center (EPIC) provides timely and expeditious information to federal, state, local, tribal, and international law enforcement agencies concerning drug interdiction and trafficking, alien and weapon smuggling, counterterrorism and other criminal activities. The systems queried include EPIC's in house computer, TECS (US Customs and Treasury), NADDIS (DEA), INS (including border crossings), FAA (Federal Aviation Association) and SENTRY-BOP.

(4) Mid-State Organized Crime Information Center (MOCIC) is part of the overall Regional Information Sharing Systems (RISS) network. This network searches multiple databases and provides access to criminal intelligence information in the region.

(5) Illinois Secretary of State (SOS) offers access to its data via LEADS. This access provides digital driver's license photographs & VISAGE Facial Recognition System data.

    (a) STIC will not store SOS information; Rather STIC will contain a link to LEADS which will, in turn, provide for access to the SOS database.

    (b) SOS data available through this link includes a subject's name, address, date of birth, gender, and digital image.

(6) The Offender Tracking System (OTS) database is managed by the Illinois Department of Corrections. OTS provides various forms of information on individuals who have been entered into the Illinois Correctional system.

(7) Illinois Department of Public Aid database provides access to information on wanted suspects, public aid and medicaid fraud, and sex offenders.

(8) The Law Enforcement Online (LEO) system is maintained by the FBI and provides a secure network that LEO members – including the law enforcement community, criminal justice officials, first responders, public safety officials, and members of the Intelligence and counterintelligence communities – can use to store, process, and transmit sensitive but unclassified information.

(9) The U.S. Department of Justice Regional Data Exchange System (RDEx) is part of the Department's Law Enforcement Information Sharing Program (LEISP). RDEx includes information to facilitate regional sharing initiatives which serves to further the LEISP's principal purpose of ensuring that criminal law enforcement information is available for users at all levels of government so that they can more effectively investigate, disrupt, and deter criminal activity, including terrorism, and protect the national security.

(10) Illinois State Police INDICES - indexed Illinois State Police case records database.

(11) Targeted Violence Information Sharing System (TAVISS) is a pointer system administered by the U.S. Secret Service National Threat Assessment Center and consists of a database of subjects who have threatened or inappropriately communicated with protectees from federal, state and local agencies.

(12) Transportation Safety Administration Federal Air Marshal Service Tactical Information Sharing System (TISS) is a database system that stores information, including photos, from suspicious activity reports, incident and arrest reports, and other sources for immediate retrieval and analysis.

(13) Financial Crimes Enforcement Network (FinCEN) is managed by the U. S. Department of Treasury and provides information to safeguard against financial crime, including terrorist financing, money laundering, and other illicit activity.

(14) Suspicious Activity Reports – STIC does not have a tips/leads hot-line system for law enforcement or the public. However, law enforcement agencies and private sector security directors may report suspicious activity directly to STIC. If the suspicious activity reported contains personally identifying information, it must meet the Collection Standards outlined in Article V, Section C of this Policy.

(15) SAFETNet – a database containing information on Illinois Department of Transportation numbers and safety inspections of commercial motor vehicles.

(16) Illinois Department of Employment Security - a database containing unemployment and tax information on employers and their personnel.

(17) Traffic Information and Planning System (TIPS) - contains information regarding prior traffic-related contacts with the ISP.

(18) Firearm Owner's Identification Database/FTIP - database used to check an individual's record of purchasing and eligibility to purchase firearms.

(19) Illinois State Police Internet Crimes Complaint database - a case tracking database used by the Internet Crimes Unit to initiate an investigation into purported internet crimes.

B. Criminal Intelligence Data Stores

STIC has two stores of criminal intelligence information – VITAL and the STIC Network Drive. Both of these systems shall comply with 28 CFR Part 23.

(1) VITAL is a data system that stores criminal justice data collected by intelligence personnel. VITAL is intended to enhance cross-jurisdictional information sharing and to facilitate crime prevention, crime fighting, and counter-terrorism efforts taking place throughout Illinois. Specifically, VITAL stores and disseminates intelligence data to assist crime investigators and patrol officers.

(a) **Entries into VITAL** – All data from any of STIC's data sources which meets the requirements of 28 CFR Part 23 may be entered into VITAL. Information that does not meet 28 CFR Part 23 collection standards is not entered into VITAL.

(b) **Downloads of VITAL** – Regularly scheduled downloads from the VITAL database to the FBI Regional Data Exchange database (R-DEx) warehouse will occur upon written agreement between ISP and the R-DEx Board.

(2) The STIC Network Drive contains both intelligence and non-intelligence information. Intelligence information will only be stored in specific folders to be designated by STIC Management. The folders containing intelligence information will be easily discernible from others in the network drive to ensure proper security and review of files contained therein.

C. Public Data Sources including Commercial Systems

Data from the following systems is not aggregated into a central database or repository. Rather, an analyst accesses each system separately to acquire relevant records related to a data subject. The ISP may contract with commercial providers to obtain this relevant data. The providers agree in writing to comply with all federal and state laws and provide quality data to industry standards. The ISP will only gather data with agency authority under state law.[17] Information will not be collected when the source agency used prohibited means to gather it.

(1) Lexis-Nexis/Accurint provides background information to government agencies on individuals, businesses, addresses, vehicles, judgments and liens, social security numbers, media news articles, among other data.

(2) Dun and Bradstreet database provides business information and is also a credit rating provider.

(3) Westlaw provides access to statutes, case law materials, public records and other legal resources, as well as current news articles and business information.

(4) National and State Sex Offender Registration Web Sites

[17] 20 ILCS 2605/2605-45(4).

(a) Intelligence personnel will have access to links to public Sex Offender Registration Web Sites.
(b) Sex offender registration information available through these links includes a registrant's name, address, physical description, and digital image along with their compliancy status, crime and the county of conviction.

(5) Federal Bureau of Prisons and State Departments of Corrections (DOC)[18] public websites provide inmate information on currently-incarcerated individuals.
(a) Intelligence personnel will have access to a link to public DOC websites.
(b) DOC information available through these links includes parent institution, inmate status, location, physical description and digital image along with sentencing information and admission, release or discharge data.

(6) Experian offers online credit reports and credit bureau data.

(7) Interpol is the largest International Police Association which facilitates cross-border police co-operation, and supports and assists all organizations, authorities and services to prevent or combat international crime.

(8) National Insurance Crime Bureau (NICB) assists law enforcement in their detection and deterrence of insurance fraud and vehicle theft.

(9) Methamphetamine Registries

D. Flow of Information

(1) **Tactical Work-Up** – This is a request for information when the requesting law enforcement officer is on an active traffic or criminal stop. The analyst conducts an abbreviated search of intelligence databases with a goal to return the relevant information to the officer within a reasonable time. Once the basic information is relayed to the officer, the analyst completes a full database work-up.
(a) LEADS, RDEx, and VITAL will be checked during every preliminary work-up. The analysts will check other relevant data sources at their discretion.

(2) **Full Database Work-Up** – The analyst determines the nature of the request, searches all relevant databases and sources of information, documents all information, and disseminates the information as appropriate.

(3) **Daily Intelligence Notes** – The analyst gathers topic information, researches and verifies that information, receives authorization from the Watch Officer, and disseminates it based upon classification.

(4) **Intelligence Alerts** – Intelligence alerts can be STIC analyst originated or pass-through products obtained by STIC from other intelligence fusion centers or sources.

[18] For purposes of this Policy, "DOC" refers to the Federal Bureau of Prisons and all state Departments of Correction.

(5) **Threat/Event Assessments** – STIC will compile background and threat information for purposes of providing assessments of events. Examples include, but are not limited to, events with large attendance expected, venues or sites of previous threats, violence or criminal activity, and those events which may have national significance.

Article VII. Authorized Persons

Section A. Authorized persons
Section B. Authorized users

A. Authorized persons

(1) For purposes of this Policy, authorized persons are Terrorism Research Specialists, Criminal Intelligence Analysts, Critical Infrastructure Specialists, Watch Officers, field intelligence personnel, public safety officials, certified police officers, and other criminal justice administrative personnel in the furtherance of their official duties.
(2) Authorized users may disseminate STIC data to authorized persons as defined in this Section only in accordance with the dissemination rules of this Policy.

B. Authorized users

(1) For purposes of this Policy, authorized users are Terrorism Research Specialists, Criminal Intelligence Analysts, Critical Infrastructure Specialists, Watch Officers, field intelligence personnel, public safety officials, certified police officers, and other criminal justice administrative personnel, who:
    (a) Are approved for STIC access by the ISP; and
    (b) Meet, at a minimum, the certification requirements for STIC access; and
    (c) Undergo training regarding the system's capabilities as well as the appropriate use and sharing of data accessed through STIC.

Article VIII. Data Quality

Section A. Ownership of data
Section B. Verifying the accuracy of STIC Law Enforcement Data Sources
Section C. Verifying the accuracy of STIC Intelligence Stores
Section D. Merged Data
Section E. Access and Review
Section F. Record Challenges

A. Ownership of data

(1) All data accessed through a law enforcement or public data source is considered to be the property of that source.
(2) Because it retains ownership of the data, each source is ultimately responsible for the quality and accuracy of its data.

(3) STIC notifies the originating agency or the originating agency's privacy officer when the center reviews the quality of the information it has received from an originating agency and identifies data that: (1) may be inaccurate or incomplete; (2) may include incorrectly merged information; (3) may be out of date; (4) cannot be verified; or (5) lacks adequate context such that the rights of the individual may be affected.
(4) Notification pursuant to Section (A)(3) above is documented via e-mail to STIC Supervisors, consistent with Article IV (A)(2)(d), who ensure the information is not entered into VITAL.
(5) All data entered into VITAL and the STIC Network Drive is deemed the property of the Illinois State Police.

B. Verifying the accuracy of STIC Law Enforcement Data Sources

Inaccurate information can have a damaging impact upon the data subject and the integrity and functional value of STIC query responses. Any information obtained through a query to STIC from Law enforcement data sources must be independently verified with the original source from which the data was extrapolated before any official action (e.g., search warrant application or arrest) is taken. Law enforcement officers and agencies are responsible for verifying the quality and accuracy of the data.

C. Verifying the accuracy of STIC Criminal Intelligence Data Stores

Any information obtained through a query to STIC from Criminal Intelligence Data Stores must be independently verified with the original source from which the data was extrapolated before any official action (e.g., search warrant application or arrest) is taken. Law enforcement officers and agencies are responsible for verifying the quality and accuracy of the data.

D. Merged Data

(1) Due to the potential harm caused by inaccurate merging of information, data about an individual from two or more sources will not be merged by a STIC Terrorism Research Specialist or Criminal Intelligence Analyst unless the identifiers or characteristics, when combined, clearly establish that the information from multiple records is about the same individual.
(2) If the matching requirements cannot fully be met but there is an identified partial match, the information may be merged only if accompanied by a statement that it has not been adequately established that the information relates to the same individual or organization.

E. Access and Review

(1) In order to avoid interference with criminal investigations, members of the public cannot access STIC or individually identifiable information on themselves or others.[19]

(2) Persons wishing to access data pertaining to themselves should communicate directly with the source of the data in question.[20]

(3) Reports regarding alleged violations and suggestions for amendments shall be submitted to the Illinois State Police Privacy Office.[21]

F. Record Challenges

Persons wishing to challenge records should communicate directly with the agency source of the data in question.

Article IX. Access and Dissemination of Law Enforcement Data Sources

Section A. Access
Section B. Dissemination

A. Access

(1) Access permissions, generally

(a) The information accessed through STIC is information that has been accessible to law enforcement officers for many years. STIC technology will permit authorized users to retrieve and analyze these same records in an efficient and timely manner as a law enforcement investigative tool.

(b) The public shall not have access to STIC data.

(2) Use for legitimate investigative purposes

(a) Information obtained from or through STIC can only be used for official law enforcement investigative purposes.

---

[19] Requests for this information are treated as Illinois Freedom of Information Act requests and will be retained consistent with that statute. *See* 5 ILCS 140.

[20] STIC will not provide these individuals with a list of sources.

[21] If an individual has a complaint or objection to the accuracy or completeness of terrorism-related information that has been or may be shared through the ISE that: (a) is held by the STIC; (b) allegedly resulted in harm to the complainant; and (c) is exempt from public disclosure, the STIC will inform the individual of the procedure for submitting, if needed, and resolving complaints or objections. Complaints will be received by Lt. Kathleen deGrasse, ISP Privacy Officer, at the following address: 9511 W. Harrison St., Des Plaines, IL 60016. The STIC will acknowledge the complaint and state that it will be reviewed, but will not confirm the existence of the information that is exempt from disclosure. If the information did not originate with the STIC, STIC will notify the originating agency in writing and, upon request, assist such agency to correct or purge any identified data/record deficiencies or to verify that the record is accurate. Any personal information originating with the STIC will be reviewed and corrected in or deleted from STIC data/records if it is determined to be erroneous, include incorrectly merged information, or be out of date. The ISP Privacy Office will maintain records of complaints and correction requests and the resulting action, if any.

(b) An official law enforcement investigative purpose means that the request for data is directly linked to a law enforcement agency's active criminal case investigation or is in response to a confirmed lead that requires additional corroboration.

B. Dissemination

(1) Prohibitions on dissemination, generally
  (a) Except as otherwise provided in this policy, information obtained from or through STIC:
    (i) Cannot be sold, published, exchanged, or otherwise disclosed, to the public or for commercial purposes; and
    (ii) Can only be disseminated to authorized persons.

(2) Confidentiality
  (a) Intelligence personnel shall protect the confidentiality of all data entered or accessed through STIC.

(3) Research purposes
  (a) The Illinois State Police may use the information accessed through STIC for research purposes in the aggregate, but such aggregate or analyzed data may not be identifiable to any person without the express consent of the individual.

(4) Secondary dissemination, generally
  (a) Authorized users may only disseminate information accessed through STIC to other authorized persons in order to fulfill their criminal justice functions.
  (b) All secondary disseminations must be logged in accordance with Article X of this Policy.

Article X. Accountability

Intelligence personnel and agencies accessing STIC data must follow all applicable state and federal laws and regulations, including rules and regulations of the Illinois State Police, regarding the use and dissemination of STIC data.

A. Programmatic audit logs

(1) Queries to VITAL will be logged by the system and identify the user initiating the query. The dissemination log must contain:
  (a) A description of the information queried (including the identity or identities to whom the information relates);
  (b) The date the information was queried;

(c) The individual who conducted the query (including their agency and contact information);
(d) The authorized person to whom the information was disseminated.

B. Secondary dissemination logs

(1) When information accessed through STIC is disseminated outside the agency from which the original request is made, a secondary dissemination log must be maintained by the disseminating agency. The dissemination log must contain:
   (a) A description of the information disseminated (including the identity or identities to whom the information relates);
   (b) The date the information was released;
   (c) The individual to whom the information was released (including their agency and contact information); and
   (d) The purpose for which the information will subsequently be used.

(2) Whenever information labeled "confidential" is disseminated outside the agency from which the original request was made, the secondary dissemination log must specify the demonstrable need to know.

C. Monitoring system use and conducting audits

(1) The Illinois State Police is responsible for monitoring the use of all STIC data sources to guard against inappropriate or unauthorized use.
(2) The Illinois State Police will investigate misuse of STIC data and conduct or coordinate audits concerning the proper use and security of STIC data by users.
(3) All STIC inquiries by authorized persons will be made available, upon request, to that authorized person's agency.

D. Violations

(1) When the Illinois State Police learn of a violation of policies, laws, or regulations concerning the use of STIC data, it must notify the chief executive of the offending agency in writing. Agencies must take action to correct such violations and provide an assurance in writing to the STIC Center Chief that corrective action has been taken.
(2) Any suspected or documented misuse of STIC information discovered by or reported to a law enforcement agency must be reported by that agency to the Illinois State Police.

E. Penalties

(1) The failure of a law enforcement agency to remedy violations may result in suspension or termination of access to STIC data.

F. ISP Statewide VITAL Coordinator

(1) The ISP will appoint a Statewide VITAL Coordinator who is responsible for training intelligence personnel in the use of VITAL and 28 CFR Part 23.

(2) The ISP Statewide VITAL Coordinator will maintain all authorized VITAL users' access forms and certification training materials at the STIC facility.

G. VITAL Quality Control

(1) The VITAL Quality Control Unit was formulated to ensure and maintain the integrity of the VITAL project database in compliance with 28 CFR Part 23.

(2) This unit has full and complete authoritative review of all information entered into the VITAL intelligence database.

(3) A second level of review shall be performed by VITAL Quality Control staff responsible for reviewing all entries of new VITAL users.

(4) All entries of new users are reviewed for the first 90 days; thereafter, Quality Control staff will randomly review 25 percent of all users' entries.

(5) Where information is found to be erroneous or deficient such that an individual's privacy rights are impacted, the VITAL Quality Control Crime Information Evaluator's responsibilities are limited to notifying the original source agency in writing for their follow-up and correction.[22]

[22] When data is obtained from that source agency, it once again goes through reliability checks prior to labeling. *See* Article V, Section D of this Policy.

Printed by the Authority of the State of Illinois
ISP Central Printing Section
Printed on Recycled Paper
ISP 5-824 (9/10) M
www.illinois.gov www.isp.state.il.us