Illinois State Police
Statewide Terrorism & Intelligence Center
Privacy Policy
Revised March 2025

Illinois State Police
Statewide Terrorism & Intelligence Center
Privacy Policy

March 2025

Article I. Purpose Statement

The mission of the Illinois State Police (ISP) Statewide Terrorism & Intelligence Center (STIC) is to provide timely, effective, and actionable intelligence information to local, state, and federal law enforcement and public safety partners in order to enhance public safety, facilitate communication between agencies, and provide support in the fight against terrorism and criminal activity, which includes all hazards. STIC is comprised of federal and state law enforcement personnel and state and public safety partners.

This Privacy, Civil Rights, and Civil Liberties (P/CRCL) Protection Policy, hereinafter referred to as policy, applies to all individuals unless otherwise specified. It describes how personally identifiable and sensitive information is collected, used, and secured by STIC. This policy was prepared by the ISP Privacy Officer and is designed to protect the privacy rights and safeguard the civil rights and civil liberties, other legal rights, and protected interests of United States (U.S.) citizens, organizations, and other specified individuals in accordance with the Privacy Act of 1974.[1]

The purpose of this policy is to promote ISP STIC and user conduct that complies with applicable federal and state law and assists the center and its users in:

- Increasing public safety and improving national security.
- Minimizing the threat and risk of injury to specific individuals.
- Minimizing the threat and risk of physical or financial 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 individual privacy, civil rights, civil liberties, and other protected interests.
- Protecting the integrity of criminal investigatory, criminal intelligence, and justice system processes and information.
- Minimizing the reluctance of individuals or groups to use or cooperate with the justice system.
- Supporting the role of the justice system in society.
- Promoting governmental legitimacy and accountability.
- Lessening the burden of the ongoing business of the justice system.
- Making the most effective use of public resources allocated to public safety agencies.

Article II. Compliance, Governance, and Oversight

All ISP STIC personnel, participating agency personnel, personnel providing information technology services to the center, staff members in other public agencies, private contractors providing services to the center, and other authorized users not employed by the center or a contractor, hereinafter referred to as intelligence personnel, will comply with the center's P/CRCL policy. This policy applies to information the center gathers or collects, receives,

[1] 5 U.S.C. § 552a

maintains, stores, accesses, discloses, or disseminates to center 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.

STIC will provide a printed or electronic copy of this policy to all center personnel, individual users, and participating agencies with acknowledgment of receipt. All intelligence personnel are required to provide acknowledgment of receipt of this policy and 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[2] and Illinois laws concerning the appropriate collection, analysis, dissemination, and retention of personally identifiable information (PII) and intelligence data.

The ISP Director has the primary responsibility for the overall operation of STIC, including, but not limited to its justice systems, operations, and coordination of personnel; the receiving, seeking, retention, evaluation, data quality, analysis, destruction, sharing, disclosure, or dissemination of information; and the enforcement of this policy is assigned to the STIC Center Chief.

The STIC Center Chief will appoint a privacy committee to review and update the privacy policy on an annual basis and perform any required audits outlined in this policy. The privacy committee is guided by a trained Privacy Officer, who is appointed by the ISP Director. The privacy committee receives reports regarding alleged errors and violations of the provisions of this policy, receives and coordinates complaint resolution under the center's redress policy, and serves as the liaison for the center, ensuring that P/CRCL protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy enhancing technologies.

Reports regarding alleged violations and suggestions for amendments shall be submitted to the privacy committee. These records will be maintained for five years. The privacy committee can be contacted at the following address: isp.sticprivacycommittee@illinois.gov. The STIC Center Chief ensures that the accountability standards outlined Article XI are adequate and enforced.

Article III. Definitions

1. **Actionable intelligence:** a relatively small piece(s) of non-obvious detail(s) that can form an initial basis point for hypothesis building.
2. **Authorized Persons:** Terrorism Research Specialists, Criminal Intelligence Analysts, Criminal Intelligence Analyst Specialists, Public Safety Program

[2] 28 Code of Federal Regulations (CFR) Part 23; 20 ILCS 2605/2605-45(4)

Managers, Center Chief, Deputy Center Chief, Assistant Center Chief, Watch Officers, field intelligence personnel, 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, Criminal Intelligence Analyst Specialists, Center Chief, Deputy Center Chief, Assistant Center Chief, Watch Officers, Public Safety Program Managers, field intelligence personnel, certified police officers, and other criminal justice administrative and intelligence personnel who meet certain qualifications outlined in this policy.
4. **Critical Infrastructure Information**: Information not customarily in the public domain and related to the security of critical infrastructure or protected systems:
    a. Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including misuse of or unauthorized access to all types of communications and data transmission systems) that violates federal, state, or local law, harms interstate commerce of the U.S., or threatens public health and safety;
    b. The ability of critical infrastructure or protected systems to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or,
    c. Any planned or past operational problem or solution regarding critical infrastructure, including repair, recovery, reconstruction, insurance, or continuity, to the extent it relates to such interference, compromise, or incapacitation.
5. **Individuals:** encompasses a single person(s) as well as any group, association, corporation, business, partnership, or other organization.
6. **Personally Identifiable Information (PII):** any data that can be used to uniquely identify, contact, or locate a single person or entity.
7. **Private Right of Action:** a term used in U.S. statutory and constitutional code for circumstances when 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.
8. **Public Safety Function:** service whose principal purpose is to protect the safety of life, health, or property. These services may be provided by state or local government entities or may be provided by non-governmental entities including, but not limited to, utility companies and other critical infrastructure industries.
9. **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, emergency

management official, public health official or member of emergency medical response organization.

10. **Private Sector Official:** Vetted official[3] with health or life safety responsibilities whose agency has signed an Infrastructure Security Awareness Non-Disclosure Agreement (NDA) with STIC.
11. **Request for Information (RFI):** a formal request (in person, telephonically, or in writing) to STIC by a public safety or private sector official for information that relates to a public safety function.
12. **Suspicious Activity:** observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity. Examples of suspicious activity include surveillance, photography of sensitive infrastructure facilities, site breach or physical intrusion, cyberattacks, testing of security, etc.[4]
13. **Suspicious Activity Report (SAR):** Official documentation of observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity. 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.
14. **U.S. Citizen:** individuals born in the U.S., 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 Customs Enforcement.
15. **Criminal Intelligence Information System (CIIS):** ISP's data system that stores criminal justice data collected by intelligence personnel.

Article IV. STIC Overview

- **A.** Intelligence Personnel
- **B.** Department of Innovation and Technology Personnel
- **C.** STIC Data Sources

A. Intelligence Personnel

1. All STIC and field intelligence personnel (hereinafter referred to as intelligence personnel) are subject to the provisions of this policy.
2. Intelligence personnel include:

[3] A security/safety check is performed on all private sector officials.

[4] Defined in the Federal Information Sharing Environment-Suspicious Activity Report (ISE-SAR) Functional Standard (Version 1.5).

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. **Criminal Intelligence Analyst Specialists** who serve as a team lead and research and analyze advanced potential criminal activity, suspect, and incident data.
d. **Public Safety Managers** who research and analyze incident data and behaviors associated with criminal activity.
e. **STIC Analytical Staff** who are any full-time ISP code employees covered by the Collective Bargaining Agreement between Council 31, American Federation of State, County and Municipal Employees (AFSCME) RC-62 and the State of Illinois, Department of Central Management Services who have obtained the job classification Criminal Intelligence Analyst, Criminal Intelligence Analyst Specialist, Terrorism Research Specialist, or Terrorism Research Trainee who provides 24 hour/7 day a week analytical support to STIC. STIC analytical staff members routinely research and analyze data in regard to criminal activity, potential incidents of terrorism, criminal and/or terrorism suspects, and incidents which may be precursors to terrorism related activities, as well as major criminal activity.
f. **STIC Work Group Members** who are any analytical staff and other criminal analyst/program coordinators assigned to STIC who provide specialized analytical research and data analysis for violent crimes, narcotics, motor vehicle theft, gaming, traffic safety, the Center for Missing and Exploited Children or any other specialization.
f. **Supervisors**
    1. **Watch Officers** provide limited supervision, direct the day-to-day operations of STIC, provide guidance and assist with the quality control function for STIC analytical staff and STIC work group members. Watch officers are sworn employees of ISP with the rank of Special Agent or Trooper.
    2. **Assistant Center Chief (ACC)** provides administrative and supervisory oversight to the Watch Officers and Public Safety Program Managers.
    3. **Deputy Center Chief (DCC)** oversees the functions of STIC and reports to the Center Chief.
    4. **Center Chief (CC)** is responsible for all functions and activities of STIC and its employees; provides administrative and supervisory oversight to the DCC and ACC.

B. Department of Innovation and Technology (DoIT) Personnel

1. Select DoIT personnel, who are supervised by the ISP Division of Justice Services, have access to information contained in law enforcement data systems and criminal intelligence data stores for the limited purpose of providing technical assistance.
2. DoIT personnel who have access to intelligence data are subject to the provisions of this policy.
3. Notwithstanding any provisions of this policy to the contrary, DoIT 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.[5]
    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

- **A.** Criminal Intelligence File
- **B.** Open Source Search
- **C.** Standards for Initiating an Intelligence Query
- **D.** Standards for Initiating an Open Source Query
- **E.** Intelligence Collection Standards/Record Entry
- **F.** Social Security Numbers and Personally Identifiable Information (PII)
- **G.** Data Quality
- **H.** Classifications
- **I.** Labeling
- **J.** Dissemination
- **K.** Review and Purge Procedures

[5] Given the availability of more modern non-intelligence information sources such as the Internet, newspapers, motor vehicle administration records, Criminal History Record Information (CHRI) , and other public record information on-line, such sources shall not be considered part of criminal intelligence systems and shall not be covered by 28 CFR Part 23, even if criminal intelligence systems access such sources during searches on criminal suspects. Therefore, criminal intelligence systems may conduct searches across the spectrum of non-intelligence systems without those systems being brought under 28 CFR Part 23.

L. Security Procedures
M. Training

STIC will seek or retain information (including "protected attributes") subject to conditions articulated below that:

- Are based on a possible threat to public safety or the enforcement of criminal law; or
- Are based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal (including terrorist) conduct or activity; or
- Are relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime, or
- Are useful in crime analysis or in the administration of criminal justice and public safety (including topical searches); and
- The source of the information is reliable and verifiable or limitations on the quality of the information is identified; and
- The information was collected in a fair and lawful manner, with the knowledge and consent of the individual, if appropriate.

The center may retain protected information that is based on a level of suspicion that is less than "reasonable suspicion," such as tips and leads (including SAR information) subject to the policies and procedures specified in this policy.

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

- Further crime prevention (including terrorism) for law enforcement, public safety, force deployment, or prosecution objectives and priorities established by the center.
- Provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal (including terrorist) activities.

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 also:
        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. Open Source Search

Open source information comes from the Internet and is available to the public. Open source data may or may not require a login identification (ID) or password. Open source information is generally obtained from, but not limited to, search engines, media, public data, social media, blogs, forums, chat rooms, as well as uploaded documents, pictures, and videos. STIC shall retain all open source search information but shall recheck its validity prior to disseminating at a later date.

C. Standards for Initiating an Intelligence Query

Intelligence personnel may perform a criminal intelligence inquiry for law enforcement officials[6] upon request and when encountering the following situations:

1. Upon a showing of reasonable suspicion of a crime;[7] or
2. Upon articulation that the query is related to an ongoing criminal investigation; or

[6] Intelligence personnel shall disseminate criminal intelligence information only to law enforcement authorities who agree to follow procedures regarding information receipt.

[7] 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.

3. For terrorism screening center encounters. Criminal predicate exists for all individuals listed on federal and international watch lists. These watch lists include, but are not limited to the following: Transportation Security Administration (TSA) No Fly List; Terrorism Screening Center (TSC) Watch List; Terrorist Identities Datamart Environment (TIDE); Terrorist Screening Database (TSDB); INTERPOL Red Notices; and the Violent Gang and Terrorist Organization File (VGTOF); or
4. For prisoner transports; or
5. Where necessary to avoid imminent danger to life or property.[8]

D. Standards for Initiating an Open Source Query

1. Intelligence personnel may perform an open source query for public safety officials and private sector officials only for a valid public safety purpose. If the official is not a law enforcement officer, the public safety or private sector official may not receive PII unless it is the result of an open source search.
2. To create STIC products (i.e., threat assessments, intelligence notes, checking critical incidents and/or major events for threats or public safety issues, etc.) for dissemination to law enforcement, public safety, or private sector officials.

E. Intelligence 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 for established length of time as defined by 28 CFR Part 23.[9]
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.

[8] A criminal intelligence inquiry may be performed, and the results may be disseminated to a government official or to any other individual, when necessary, to avoid imminent danger to life or property. 28 CFR Part 23.20(f)(1) and (f)(2)

[9] 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.

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[10] 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.[13]
8. Factors such as race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity must not be considered as creating suspicion. However, those attributes may be documented in specific suspect descriptions for identification purposes.
9. 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.
10. 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. 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, 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.
11. If the information gathered pertains to First Amendment-protected activities, there must be:
    a. Reasonable belief that violence or the destruction of property will occur;
    b. Reasonable indications of criminal activity;
    c. Potential threats towards the protest groups; or
    d. Collection must be necessary to maintain public safety. Once the event has concluded, if there is no criminal activity or criminal predicate the information shall not be retained in the criminal intelligence stores.

F. Social Security Numbers and Personally Identifiable Information (PII)

1. Intelligence personnel may not collect, use, or disclose a social security number or other types of PII which may include date of birth, phone numbers, addresses, email accounts, driver's license numbers, bank account numbers, and other information which could disclose the identity of the person except in the following instances:
    a. To agents, employees, contractors, or subcontractors of a governmental entity or disclosure by a governmental entity to another governmental entity or its agents, employees, contractors, or subcontractors if disclosure is necessary in order for the entity to perform its duties and responsibilities;

[10] Non-criminal identifying information is information that pertains to an individual, organization, group, or business that is not suspected of criminal involvement, but the information is relevant to a criminal suspect. [13] The 1998 Policy Clarification to 28 CFR Part 23.

and, if disclosing to a contractor or subcontractor, prior to such disclosure, the governmental entity must first receive from the contractor or subcontractor a copy of the contractor's or subcontractor's policy that sets forth how the requirements imposed under Identity Protection Act (5 ILCS 179/) on a governmental entity to protect an individual's social security number will be achieved;

b. Pursuant to a court order, warrant, or subpoena;

c. To ensure the safety of state and local government employees; persons committed to correctional facilities, local jails, and other law enforcement facilities or retention centers; wards of the state; and all persons working in or visiting a state or local government agency facility; or

d. For internal verification or administrative purposes.

2. Any other collection, use or disclosure of a social security number pursuant to 5 ILCS 179/1 must be approved by the STIC Assistant Center Chief, Deputy Center Chief, or Center Chief**.**

G. 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. STIC personnel will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources; is accurate, current, and complete; and is relevant to the persons or organization to which it is attributed.

3. If intelligence personnel have cause to believe the data contains an error or deficiency, they must contact the ISP statewide CIIS coordinator for confirmation with the source of the data.

4. Random criminal intelligence information audits are performed on a continual basis by ISP statewide CIIS coordinator.

5. 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.

6. The ISP CIIS maintains a record of the source of the information.[11]

[11] *Supra* note 13.

7. 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.
8. A data element with a source reliability of "unknown" and a validity assessment of "unknown" may not be entered into an intelligence system.
9. 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 affected, provide notice to authorized users who are known to have received the information.[12]

H. Classifications

1. Prior to entering information into any intelligence system, intelligence personnel shall portion mark 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 same level of privacy protection. Portion marking also indicates whether internal approval must be completed prior to the release of the information to persons outside STIC.
2. STIC portion marks data into the following categories:
    a. **Controlled Unclassified Information (CUI)** is sensitive, unclassified information that requires safeguarding and controls on dissemination, as mandated by laws, regulations, or government-wide policies, and is not publicly releasable without authorization.
    b. **Confidential** is the highest level of unclassified but sensitive information. Access to information defined as "confidential" is limited, even among law enforcement officers.
    c. **Law Enforcement Sensitive (LES)** is middle level unclassified but sensitive information. LES may contain PII and may be disseminated to law enforcement personnel only.
    d. **For Official Use Only (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 does not contain dates of birth or social security numbers. FOUO may contain an individual's photo but only where

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

that photo relates to the individual's record of conviction.[13] FOUO may not be released to the general public.

e. **Protected Critical Infrastructure Information (PCII)** is a subset of Critical Infrastructure Information for which protection is requested under the PCII program by the requestor. PCII may not be released to the general public.

f. **Open Source** is any information that is publicly available. This information will be marked as "Unclassified" using an indicator of (U). Open source information may not be released to the general public.

3. **Portion Marking:** All intelligence information has its portion marking directly on the information file.
4. **Re-evaluation of Portion Marking:** 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.

I. Labeling

1. The data contained within STIC criminal intelligence systems will be identified as intelligence or non-criminal identifying information and any applicable legal requirements for handling such data indicated as provided in Article V, Section E of this policy.
2. At the time a decision is made to retain information, it will be labeled to the maximum extent feasible, pursuant to applicable limitations on access and sensitivity of disclosure in order to:
    - Protect confidential sources and police undercover techniques and methods.
    - Not interfere with or compromise pending criminal investigations.
    - Protect an individual's right of privacy and his or her civil rights and civil liberties.
    - Provide legally required protections based on the individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, recipient of mental health or developmental disabilities services, or resident of a domestic abuse shelter.
3. All criminal intelligence information disseminated will be labeled as such so that the recipient may handle the information in accordance with applicable legal requirements.
4. Information labeled as non-criminal identifying information will be maintained and disseminated in the same manner as intelligence information.
5. The labels assigned to existing information will be re-evaluated whenever:
    - New information is added that has an impact on access limitations or the sensitivity of disclosure of the information.

[13] Training materials used for training purposes may contain an individual's photo that does not relate to the individual's record of conviction.

- There is a change in the use of the information affecting access or disclosure limitations.

J. 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 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.[14]
3. Intelligence personnel may disseminate a threat assessment of criminal intelligence information to any individual where necessary to avoid imminent danger to life or property.[15]
4. Recipients on STIC's distribution lists must have a signed NDA on record with STIC.
5. 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.
6. Secondary dissemination of STIC data is permissible provided the dissemination would have been allowable directly from STIC systems under the terms of this policy.
7. FOUO, PCII, and open source information contained within the threat assessment may be disseminated outside law enforcement only to authorized individuals with a need and a right to know the information.

[14] 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.

[15] 28 CFR Part 23.20(f)(2) provides that criminal intelligence information may be disseminated "to a government official or to any other individual, when necessary, to avoid imminent danger to life or property."

K. Review and Purge Procedures[16]

1. Intelligence personnel will make every reasonable effort to ensure that information maintained in intelligence systems is current, accurate, and relevant. 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 noncriminal 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.[17]
5. Information removal must be approved by the STIC Center 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 retention period.
7. Non-criminal identifying information will be maintained and/or destroyed in accordance with the Illinois State Records Act.[21]

L. Security Procedures

STIC has formally adopted the Criminal Justice Information Systems (CJIS) Security Policy of the U.S. Department of Justice, Federal Bureau of Investigation (FBI), Criminal Justice Information Services Division and applies these provisions to STIC operations. STIC will develop a separate security policy. Firewalls are in place to prevent unauthorized agencies or entities from accessing STIC resources. 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 CIIS**.**

1. Role-based user access: intelligence systems that intelligence personnel access utilizes various levels of role-based user access.

- **a.** Each user's role shall determine the types of information accessible to the user.
- **b.** Each user's role contains certain permissions to modify or delete records.

2. **Security breaches and security breach notification:** ISP will monitor and respond to security breaches or breach attempts.[18]

---

[16] 28 CFR Part 23; 20 ILCS 2605/2605-45(4).

[17] Electronic records are permanently deleted, and paper files are shredded.

[21] 5 ILCS 160/1 et seq.

[18] See 815 ILCS 530/1 et seq.

a. In the event that intelligence personnel become aware of a breach of the security of unencrypted personal information, ISP will notify the individual whose personal information was or is reasonably believed to have been obtained and accessed, 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.

3. **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.
4. **Disaster Recovery:** ISP has appropriate disaster recovery procedures for STIC data outlined in ISP's Disaster Recovery Plan.
5. **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.
6. **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.

M. Training

1. Personnel Training

a. STIC has adopted the Department of Homeland Security (DHS) standards as the education and training standard for its Terrorism Research Specialists, Criminal Intelligence Analysts, Criminal Intelligence Analyst Specialists, and Public Safety Program Managers.

b. All intelligence personnel are provided training on this policy.

c. ISP Division of Justice Services personnel who have access to STIC data are provided training on this policy.

d. Training is provided on this policy to all intelligence personnel, including Watch Officers and management (Center Chief and Assistant Center Chiefs).

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 minimally has completed training regarding the Privacy Act of 1974 and 28 CFR Part 23.

g. Private sector personnel in contractual relationships with ISP STIC will receive training on this policy.

h. All intelligence personnel with access to social security numbers in the course of performing their duties will be trained on ISP's Identity Protection Policy pursuant to the Identity Protection Act.[19]

2. Policy Awareness

a. This 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 policy.

3. Policy Updates

a. The ISP Privacy Officer will update this policy as new information sources are accessed through STIC.

b. The ISP Privacy Officer will monitor legislative activity and update this policy accordingly.

c. The ISP Privacy Officer will review this 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

B. Criminal Intelligence Data Stores

C. Public Data Sources including Commercial Systems

D. Flow of Information

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 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 ISP, 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).

[19] Illinois State Police Directive SRV-200 – Information Security and Disposal of Personal Information.

2. **CrimePad** is a records management system for the Division of Criminal Investigation and the Division of Forensic Services.
3. **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.
4. **DocuWare** is a cloud-based document management and workflow automation software solution that helps digitize, secure, and manage documents.
5. **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 (U.S. Customs and Treasury); NADDIS (DEA); ICE (including border crossings); FAA (Federal Aviation Association), and SENTRY-BOP.
6. **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.
7. **Illinois SOS** offers access to its data via LEADS. This access provides digital driver's license photographs.
    a. STIC will not store SOS information, but 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.
    c. STIC can request facial recognition through SOS's internal system. Facial recognition will only be completed in accordance with 28 CFR Part 23 and the procedures outlined in this policy.
8. The **Offender 360 (O360)** database is managed by the Illinois Department of Corrections (DOC). O360 provides various forms of information on individuals who have been entered into the Illinois correctional system.
9. **Illinois Department of Human Services' database** provides access to employment.
10. The **Law Enforcement Enterprise Portal Online (LEEP)** system is maintained by the FBI and provides a secure network that LEEP 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.
11. ISP **INDICES** is a database that contains indexed ISP case records.
12. **Protective Intelligence Exchange (PIX)** 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.

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. STIC does not have a tips/leads hot-line system for law enforcement or the public for SAR**s.** However, law enforcement agencies and private sector security officials 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. **Federal Motor Carrier Safety Administration (FMCSA)** is a database containing information on U.S. Department of Transportation numbers and safety inspections of commercial motor vehicles.
16. **Firearm Owner's Identification Database/FTIP** database is used to check an individual's record of purchasing and eligibility to purchase firearms.
17. **TraCS** is a repository for ISP report management.
18. A **deconfliction** is a repository of event-driven criminal investigations.
19. **Homeland Security Information Network (HSIN)** is a nationally secure and trusted Web-based portal for information sharing and collaboration among federal, state, local, tribal, territorial, private sector, and international partners engaged in the homeland security mission.
20. **National Data Exchange (N-DEx)** is a repository of criminal justice records, available in a secure online environment, managed by the FBI's Criminal Justice Information Services (CJIS) Division.
21. **Joint Automated Booking System (JABS)** is an information-sharing system as well as a conduit for sending standard booking data directly to the FBI's Integrated Automated Fingerprint Identification System (IAFIS). JABS receives common offender data elements (biographical data, fingerprints, and photographs) from automated booking stations and booking systems of DOJ law enforcement components and certain other federal law enforcement agencies and maintains a shared repository that can be accessed by all participating agencies.
22. **Regional Justice Information Service (REJIS)** provides record management services to law enforcement, courts, corrections, and government agencies as well as private security and legal firms at the local, state, and federal levels.

B. Criminal Intelligence Data Stores

STIC has two stores of criminal intelligence information: the STIC CIIS and the STIC network drive. Both of these systems shall comply with 28 CFR Part 23.

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

a. **Entries into the STIC CIIS:** All data from any of STIC's data sources which meets the requirements of 28 CFR Part 23 may be entered into the CIIS. Information that does not meet 28 CFR Part 23 collection standards is not entered into the CIIS
b. **Downloads of the CIIS:** Regularly scheduled downloads from the database to the FBI Regional Data Exchange database (N-DEx) warehouse may occur upon written agreement between ISP and the N-DEx Board.

2. The STIC network drive contains both intelligence and non-criminal identifying 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. 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. ISP will only gather data with agency authority under state law.[20] Information will not be collected when the source agency used prohibited means to gather it.

1. **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. **Federal Bureau of Prisons and State DOC**[21] 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.
3. **Interpol** is the largest International Police Association which facilitates cross-border police cooperation, and supports and assists all organizations, authorities, and services to prevent or combat international crime.
4. **National Insurance Crime Bureau (NICB)** assists law enforcement in their detection and deterrence of insurance fraud and vehicle theft.
5. **TLO** is an online investigation service and commercial public records database.
6. The **Internet** has the capability of researching full Internet sources including commercial, educational, and governmental networks.

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

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

D. Flow of Information

1. Work-ups

a. **A 20-minute (tactical) work-up** 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.

   1. LEADS, N-DEx, and the STIC CIIS will be checked during every tactical work-up. The analysts will check other relevant data sources at their discretion.

2. **A full database work-up** occurs when 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. Analytical Products

a. **Intelligence notes** are created by STIC analysts. The analyst gathers topic information, researches and verifies that information, receives authorization from the watch officer, and disseminates it to partners based upon the portion marking of the information.

b. **Intelligence alerts** (also known as officer safety alerts) can be STIC analyst originated or pass-through products obtained by STIC from other intelligence fusion centers or sources. Intelligence alerts are not disseminated to the general public.

c. **Threat assessments** are completed by compiling background and threat information for purposes of providing assessments of special events or critical infrastructure. 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. FOUO, PCII, and open-source information contained within the threat assessment may be disseminated outside law enforcement within the restrictions of this policy. STIC will not complete intelligence work-ups on individuals unless reasonable suspicion exists that the subject in question is involved in criminal activity and that suspected criminal activity has a bearing on the event involved.

d. **Be on the lookout (BOLOs)** will be disseminated at the request of officers in the field. A suspect's PII will be included in a BOLO when reasonable suspicion exists that the subject in question is involved in criminal activity. A missing person's PII will be included in a BOLO when that person is missing under unexplained, involuntary, or suspicious circumstances. BOLOs are not entered into LEADS and are only disseminated to law enforcement officers.

e. Intelligence notes and threat assessments must be reviewed and approved by the ISP Privacy Officer to ensure they adhere to appropriate P/CRCL protections prior to dissemination and sharing by the center.

Article VII. – Suspicious Activity Reports (SARs)

- **A.** Standards for Initiating a Query of the Information Sharing Environment (ISE)-SAR Database
- **B.** Collection Standards/Record Entry
- **C.** Dissemination
- **D.** Security Procedures
- **E.** Applicability

Intelligence personnel are required to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of SAR information. The search, collection, and dissemination restrictions to SAR information outlined in this article are only applicable to that information which contains PII as defined in Article III, Section 6 of this policy. A SAR is an official documentation of observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity.

A. Standards for Initiating a Query of the Information Sharing Environment (ISE)-SAR Database

1. Intelligence personnel may perform a SAR inquiry for law enforcement officials upon request and upon a showing of reasonable suspicion of a crime.
2. Intelligence personnel may perform a SAR inquiry, upon request, where necessary to avoid imminent danger to life or property.
3. Prior to allowing access to the SAR information, intelligence personnel shall:
    - **a.** Ensure that attempts to validate or refute the information have taken place;
    - **b.** Ensure that the information has been assessed for sensitivity and confidence by subjecting it to an evaluation or screening process to determine its credibility and value; and
    - **c.** Categorize the information as unsubstantiated or uncorroborated if attempts to validate or determine the reliability of the information have been unsuccessful.
4. Intelligence personnel will only search SAR information which meets the reasonable suspicion standard and is marked as such.
5. Intelligence personnel will use a standard reporting format and data collection codes for SAR information.
6. While STIC does not accept tips, leads, and SARs from the general public, STIC will accept SAR reporting and information from public safety partners which have been vetted and are part of the STIC public safety outreach programs. Any such SAR information and results of inquiries will not be shared by STIC with the public safety partners but may be accessed through their local law enforcement jurisdictions where appropriate.

B. Collection Standards/Record Entry

1. Intelligence personnel are responsible for documenting SAR information into the STIC CIIS.
2. Intelligence personnel shall store only SAR information that meets 28 CFR Part 23 collection standards and is marked as such and which includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other types of information.
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 may retain SAR information for a period up to five years and shall assign a "disposition" label (for example, undetermined or unresolved, cleared or unfounded, verified, or under active investigation). This disposition label must be attached to the SAR information within one year after it is entered into the database so that a subsequently authorized user knows the status and purpose for the retention. STIC will retain the information based on the retention period associated with the disposition label.
5. If the disposition label is "cleared or unfounded," that SAR information which contains PII will be immediately purged from the ISE-SAR database or, at a minimum, the PII will be removed from the SAR file.
6. STIC'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.
7. Law enforcement officers and appropriate STIC and participating agency staff will be trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism.

C. Dissemination

Intelligence personnel shall:

1. Disseminate only SAR information that rises to the level of reasonable suspicion.
2. Disseminate SAR information in response to an interagency inquiry for law enforcement, homeland security, or public safety and analytical purposes or provide an assessment of the information to any agency, entity, individual, or the public when credible information indicates an imminent danger to life or property.

3. Disseminate SAR 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.[22]
4. Allow for secondary dissemination of SAR information provided the dissemination would have been allowable directly from STIC systems under the terms of this policy.

D. Security Procedures

1. STIC will adhere to and follow STIC's physical, administrative, and technical security measures to ensure the protection and security of SAR information. SAR information will be secured in a system that is the same as or similar to the system that secures criminal intelligence.

2. STIC will secure SAR information in a separate repository system using security procedures and policies that are the same as or similar to those used for a system that secures data rising to the level of reasonable suspicion under 28 CFR Part 23.
3. STIC incorporates the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious activities and incidents (SAR process) into existing processes and systems used to manage other crime-related information and criminal intelligence, thus leveraging existing policies and protocols utilized to protect the information and P/CRCL.
4. STIC'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 (race, religion, national origin, ethnicity, etc.) and civil liberties (speech, assembly, religious exercise, etc.) will not be intentionally or inadvertently gathered, documented, processed, and shared.
5. STIC adheres to the current version of the ISE-SAR functional standard for its SAR process, including the use of a standard reporting format and commonly accepted data collection codes and a sharing process that complies with the ISE-SAR functional standard for suspicious activity potentially related to terrorism.
6. STIC will share any SAR reports that may reasonably be indicative of terrorist or criminal activity through the use of the eGuardian system.[23] Through eGuardian, SARs can be reported to the FBI for action and can also be shared with other law

[22] *Supra* note 15.

[23] eGuardian is utilized to share any SARs which need evaluation and possible investigations with the appropriate regional office of the FBI.

enforcement agencies as part of the ISE. Any SAR which meets the requirements but could have a reasonable explanation will not be shared in the ISE[24] but only reported.

The general provisions of this policy apply unless otherwise provided for in this article.

E. Applicability

Article VIII. Authorized Persons and Users

- **A.** Authorized Persons
- **B.** Authorized Users

A. Authorized Persons

1. For purposes of this policy, authorized persons are Terrorism Research Specialists, Criminal Intelligence Analysts, Criminal Intelligence Analyst Specialists, Center Chief, Deputy Center Chief, Assistant Center Chief, Watch Officers, Public Safety Program Managers, 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, Criminal Intelligence Analyst Specialists, Center Chief, Deputy Center Chief, Assistant Center Chief, Watch Officers, Public Safety Program Managers, field intelligence personnel, public safety officials, certified police officers, and other criminal justice administrative personnel, who:
    - **a.** Are approved for STIC access by ISP; and
    - **b.** Meet, at a minimum, the certification requirements for STIC access; and undergo training regarding the system's capabilities as well as the appropriate use and sharing of data accessed through STIC.

Article IX. Data Quality

- **A.** Ownership of Data
- **B.** Verifying the Accuracy of STIC Law Enforcement Data Sources
- **C.** Verifying the Accuracy of STIC Criminal Intelligence Stores
- **D.** Merged Data
- **E.** Access and Review

[24] Information shared in the ISE must include certain descriptive information to include the center's name, the date the information was collected, the title and contact information for the person to whom questions should be directed, and any restrictions on the sharing of the information based upon sensitivity or classification.

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:
    - **a.** May be inaccurate or incomplete;
    - **b.** May include incorrectly merged information;
    - **c.** May be out of date;
    - **d.** Cannot be verified; or
    - **e.** 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 V (G) who ensure the information is not entered into the ISP CIIS.

   All data entered into the STIC CIIS and the STIC network drive is deemed the property of ISP.
5. Any connections to the STIC CIIS must allow for intelligence personnel to edit, alter, or remove information pursuant to this policy.

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 response. 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, Criminal Intelligence Analyst, or Criminal Intelligence Analyst Specialist unless the identifiers or characteristics, when combined, clearly establish that the information from multiple records is about the same individual or organization.

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.[25]
2. Persons wishing to access data pertaining to themselves should communicate directly with the source of the data in question.[26]

3. Reports regarding alleged violations and suggestions for amendments shall be submitted to the ISP Privacy Committee.[27]

F. Record Challenges

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

Article X. Access and Dissemination of Law Enforcement Data Sources

A. Access
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.

---

[25] Requests for this information are treated as Illinois Freedom of Information Act requests and will be handled consistent with that statute. See 5 ILCS 140/1, et seq.

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

[27] 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 STIC; (b) allegedly resulted in harm to the complainant;

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:
  - **1.** Cannot be sold, published, exchanged, or otherwise disclosed, to the public or for commercial purposes; and
  - **2.** 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.** ISP 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.

5. 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.

6. STIC shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information unless otherwise required by law.

Article XI. Accountability

A. Programmatic Audit Logs
B. Secondary Dissemination Logs
C. Monitoring System Use and Conducting Audits
D. Violations
E. Penalties
F. ISP Statewide CIIS Coordinator
G. ISP Statewide CIIS Quality Control

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

A. Programmatic Audit Logs

1. Queries to the ISP CIIS 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 marked "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. ISP is responsible for monitoring the use of all STIC data sources to guard against inappropriate or unauthorized use. ISP will investigate misuse of STIC data and conduct or coordinate audits concerning the proper use and security of STIC data by users.

---

and (c) is exempt from public disclosure, STIC will inform the individual of the procedure for submitting, if needed, and resolving complaints or objections. Complaints will be received by the ISP Privacy Committee, at the following address: isp.sticprivacycommittee@illinois.gov. 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 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 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 out of date. The ISP Privacy Committee will maintain records of complaints and correction requests and the resulting action, if any.

2. All STIC inquiries by authorized persons will be made available, upon request, to that authorized person's agency.

D. Violations

1. When ISP learns 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 ISP.

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 CIIS Coordinator

1. ISP will appoint a CIIS coordinator who is responsible for training intelligence personnel in the use of CIIS and 28 CFR Part 23.
2. The ISP CIIS coordinator will maintain all authorized CIIS users' access forms and certification training materials at the STIC facility.

G. ISP CIIS Quality Control

1. The ISP CIIS quality control was formulated to ensure and maintain the integrity of the CIIS in compliance with 28 CFR Part 23.
2. The ISP CIIS quality control has full and complete authoritative review of all information entered into the ISP CIIS.
3. A second level of review shall be performed by ISP CIIS quality control staff responsible for reviewing all entries of new 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 ISP CIIS quality control responsibilities are limited to notifying the original source agency in writing for their follow-up and correction.[28]

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