Indiana Intelligence Fusion Center

Privacy Policy

February 1, 2026

INDIANA INTELLIGENCE FUSION CENTER
PRIVACY POLICY

TABLE CONTENTS

A. PURPOSE

The mission of the Indiana Intelligence Fusion Center (IIFC) is to collect, evaluate, analyze, and disseminate information and intelligence data (records) regarding criminal and terrorist activity in the State of Indiana while protecting privacy, civil rights, civil liberties, and other protected interests. This includes implementing appropriate privacy and civil liberties safeguards as outlined in the principles of the Privacy Act of 1974, as amended, to ensure that the information privacy and other legal rights of individuals and organizations are protected. The information and intelligence data collected, evaluated, and analyzed will be disseminated by the IIFC to members of the law enforcement and public safety communities responsible for the prevention, mitigation, and response to crime and terrorism.

This policy is intended to protect privacy, civil rights, and civil liberties:

- Increasing public safety and improving national security.
- Minimizing the threat and risk of injury to all individuals.
- Protecting the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information.

The IIFC recognizes the importance of ensuring the protection of individual constitutional rights, civil liberties, civil rights, and privacy interests throughout the intelligence and investigatory process.

B. POLICY APPLICABILITY and LEGAL COMPLIANCE

All IIFC personnel, participating agency personnel, information technology personnel providing services to the agency, private contractors, and other authorized users will comply with the IIFC's privacy policy, civil rights and civil liberties, the information the center collects, receives, maintains, archives, accesses, or discloses, or disseminates to center personnel, governmental agencies (including Information Sharing Environment (ISE) participating agencies), and participating justice and public safety agencies, as well as to private contractors and the general public.

The IIFC will provide an electronic copy of this policy to all IIFC personnel and any interested persons via the IIFC website.

C. GOVERNANCE and OVERSIGHT

Primary responsibility for the operation of the IIFC, its justice systems, operations, and coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing, or disclosure of information; and the enforcement of this policy is assigned to the IIFC Administrator, who also must adhere to all enforcement procedures outlined in this policy.

IIFC privacy compliance is guided by a trained Privacy Officer who is appointed by the IIFC Administrator. Violations of the privacy policy can be reported to the IIFC Administrator or to the Privacy Officer. Reporting can be made in person, in writing or via any electronic communication.

D. DEFINITIONS

The primary terms and definitions used in this privacy policy are set forth in Appendix A- Definitions.

E. INFORMATION QUALITY ASSURANCE

The Indiana Intelligence Fusion Center may collect criminal intelligence information only if:

- Reasonable suspicion exists that the subject of the criminal intelligence information is involved with or has knowledge of possible criminal or terrorist activity; and
- The criminal intelligence information is relevant to the criminal or terrorist activity.

IIFC personnel are required to adhere to the ISE- SAR Functional Standard and state and federal laws for the receipt, collection, assessment, storage, access, dissemination, retention, and security of Suspicious Activity Reporting (SAR) information.

Subject to the policies and procedures specified in this policy, the IIFC may retain information, such as tips and leads or suspicious activity report (SAR) information, based on suspicion that behaviors are reasonably indicative of pre-operational planning associated with terrorism.

- The ISE-SAR Functional Standard *does not alter law enforcement officers' constitutional obligations when interacting with the public*. This means, for example, that constitutional protections and agency policies and procedures that apply to a law enforcement officer's authority to stop, stop and frisk ("Terry Stop"), request identification, or detain and question an individual apply in the same measure to observed behavior *that is reasonably indicative of pre-operational planning associated with terrorism*. It is also important to recognize that many terrorism-related activities are now being funded via local or regional criminal organizations whose direct association with terrorism *may be tenuous*. This places law enforcement and homeland security professionals in the unique, yet demanding, position of identifying suspicious behaviors *as a by-product or secondary element in a criminal enforcement or investigative activity*.

The IIFC 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, as well as constitutional rights, including personal privacy and other civil liberties, and civil rights.

The IIFC will not seek or retain and information-originating agencies will agree not to submit, information about individuals or organizations solely on the basis of their race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation; nor religious, political, social views, or activities; nor their participation in a particular noncriminal organization or lawful event.

The IIFC applies restriction labels to all disseminated information released to an authorized user, and ensures that any agency-originated information has also applied appropriate restriction labels. The labels pertain to the following:

- The information pertains to all individuals pursuant to IC 10-11-9-4, and
- The information is subject to Federal and Indiana state laws restricting access, use, or disclosure, including, but not limited to, 18 USC 2721, IC 35-38-9 et seq., IC 31-39-8 et seq., IC 4-1-10 et seq., IC 5-2 et seq., IC 5-14-3 et seq., and 28 CFR Part 23.

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

- The reliability of the source (for example, reliable, usually reliable, unreliable, unknown); and
- The validity of the content (for example, confirmed, probable, doubtful, cannot be judged).

At the time a decision is made to retain information, it will be labeled (by record, data set, or system of records), to the maximum extent feasible, pursuant to applicable limitations on access and sensitivity of disclosure to:

- Not interfere with or compromise pending criminal investigations.
- Protect an individual's right of privacy, civil rights, and civil liberties;

The IIFC will identify and review information that is originated by the IIFC prior to sharing that information in the ISE.

The IIFC will keep a record of the source of all information retained by the agency in accordance with federal guidelines and state law.

The IIFC will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources of information; accurate; current; complete, including the relevant context in which it was sought or received and other related information; and merged with other information about the same individual or organization only when the applicable standard has been met.

At the time of retention in the system, the information will be labeled regarding its level of quality.

The labeling of retained information will be reevaluated when new information is gathered that has an impact on the confidence (validity and reliability) of the previously retained information.

The IIFC investigates in a timely manner and will make every reasonable effort to ensure that information will be corrected, deleted from the system, or not used when the agency/center learns that the information is erroneous, misleading, obsolete, or otherwise unreliable; the source of the information did not have authority to gather the information or to provide the information to the agency; or the source used prohibited means to gather the information, except when the source did not act as an agent to a bona fide law enforcement officer.

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

F. TRAINING

The IIFC will require all assigned personnel of IIFC to participate in training programs regarding implementation of and adherence to the IIFC's privacy, civil rights, and civil liberties policy.

All personnel assigned to the IIFC shall be required to annually take 28 CFR Part 23 training.

The IIFC will provide special training to personnel authorized to share protected information through the ISE regarding the IIFC requirements and policies for collection, use, and disclosure of protected information.

The IIFC privacy policy training program will cover:

- Purposes of the privacy, civil rights, and civil liberties protection policy;
- Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the IIFC;
- How to implement the policy in the day-to-day work of the user, whether a paper or systems user;
- The impact of improper activities associated with infractions within or through the agency;
- Mechanisms for reporting violations of agency/center privacy-protection policies; and
- The nature and possible penalties for policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.

G. SHARING and DISCLOSURE

Access to or disclosure of records retained by the IIFC will be provided only to persons within other governmental agencies or private sector entities who are authorized to have access and only for legitimate law enforcement, public protection, public prosecution, public health, or justice purposes and only for the performance of official duties in accordance with laws and procedures applicable to the agency for which the person is working. An audit trail will be kept listing anyone accessing and/or receiving information.

Agencies external to the IIFC may not disseminate IIFC information received from IIFC without approval from the originator of the information. This requirement does not apply to information that was already provided to, disclosed to, or independently acquired by, the IIFC without restrictions from its originating source. The external agencies may be required to obtain approval from the IIFC to disseminate the information received from the IIFC as needed.
Records retained by the IIFC may be accessed or disseminated to those responsible for public protection, safety, or public health only for public protection, safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures. An audit trail sufficient to allow the identification of each individual who accessed or received information will be kept.

Information gathered and records retained by the IIFC may be accessed or disseminated for specific

purposes upon request by persons authorized by law to have such access and only for those users and purposes specified in the law. An audit trail will be kept for a minimum of three (3) years of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.

Information gathered and records retained by the IIFC may be accessed or disclosed to a member of the public only if the information is defined by law to be a public record or otherwise appropriate for release to further the IIFC mission and is not exempt from disclosure by law. Such information may be disclosed only in accordance with the laws of the State of Indiana for this type of information. An audit trail will be kept of all requests and of what information is disclosed to a member of the public.

Information gathered and records retained by the IIFC will not be:

- Sold, published, exchanged, or disclosed for commercial purposes.
- Disseminated to persons not authorized to access or use the information.

There are several categories of records that will ordinarily not be provided to the public under the Indiana Access to Public Records Act. This includes, but is not limited to:

- Records required to be kept confidential by law are exempted from disclosure requirements under IC 5-14-3-4.
- Investigatory records of law enforcement agencies are exempted from disclosure requirements under IC 5-14-3-4 (b)(1); however, certain law enforcement records must be made available for inspection and copying under IC 5-14-3-5.
- Criminal Intelligence Information pursuant to IC 5-2-4-6 is declared criminal confidential and exempted from the Indiana Access to Public Records Act (IC 5-14-3-4(b) at the discretion of a public agency, unless access to the records is specifically required by a state or federal statute or is ordered by a court under the rules of discovery.
- A record or part of a record the public disclosure of which would have a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack is exempted from disclosure requirements under IC 5-14-34(b)(19).
- Protected federal, state, local, or tribal records, which may include records originated and controlled by another agency that cannot be shared without permission, unless they are required to be disclosed under the Indiana Access to Public Records Act. Participating agencies providing data remain the owners of the data contributed and, as such, are responsible for granting access when required by applicable federal or state law or court order.
- Subject only to the requirement of IIFC to comply with the Indiana Access to Public Records Act or other applicable law, the IIFC shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.
- IIFC participating agencies providing data remain the owners of the data contributed to the IIFC. The IIFC may be required by statute, regulation, or mutual agreement to use or disseminate the data in a particular manner. Members of the public can access individually identifiable information on themselves from the IIFC, as permissible by law, by making a request under the Indiana Access to Public Records Act or other law permitting access, or by making a request to the originating agency. Persons wishing to access data pertaining to themselves should

communicate directly with the agency or entity that is the source of the data. Citizen inquiries to the IIFC about personal data are the responsibility of the Indiana State Police Legal Department. The IIFC Assistant Director will notify the agency who is the owner or originator of the data of the request. The agency shall designate in writing to the IIFC which of those records, if any, the agency considers confidential information or otherwise exempted from disclosure under exceptions to the Indiana Access to Public Records Act set forth in IC 5-14-34. The IIFC shall promptly review the basis for the agency's claims, including claims of confidentiality under federal laws, and shall not disclose the records subject to the agency's claims if the IIFC concurs with the agency's claims. If the IIFC determines that its obligations under the Indiana Access to Public Records Act requires such disclosure, the IIFC shall promptly notify the agency of such determination and will not make such disclosure if the agency obtains, prior to the expiration of the applicable timeframe to respond to such request, either an opinion from the Indiana Public Access Counselor that such disclosure is not required, or a protective order or other relief from any court of competent jurisdiction preventing such disclosure. This must be done in sufficient time to permit IIFC compliance with deadlines found with IC 5-14-3-9.

- Participating agencies agree that they will notify owners of the information of requests related to individually identifiable information.
- Upon receipt of a request for one or more documents under the Indiana Access to Public Records Act, IIFC personnel will immediately contact an attorney in the Indiana State Police Legal Department for assistance in responding to the request. A prompt response is required under Indiana Law, with very short deadlines which vary depending upon the circumstances of the request for records.

H. REDRESS

H.1 DISCLOSURE

Upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity.

An individual is entitled to know the existence of and to review the information about him or her that has been gathered and retained by the IIFC. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information. The IIFC's response to the request for information will be made within a reasonable time and in a form that is readily intelligible to the individual. A record will be kept of all requests and of what information is disclosed to an individual.

Pursuant to the IIFC's lawful discretion, the existence, content, and source of the information will not be made available to an individual, unless required under the Indiana Access to Public Records Act or other law, when:

- Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution.
- Disclosure would endanger the health or safety of an individual, organization, or community.
- The information is in a criminal intelligence system;
- The information is classified under federal law;
- The information source does not reside with the IIFC; or

- The IIFC did not originate or does not have a right to disclose the information.

If the information does not originate with the entity, the requestor will be referred to the originating agency.

H.2 COMPLAINTS and CORRECTIONS

If an individual has complaints or objections to the accuracy or completeness of information about him or her originating with the IIFC, including information that may be shared through the ISE, the IIFC's Privacy Officer or legal counsel will inform the individual of the procedure for submitting complaints or requesting corrections. A record will be kept of all complaints and requests for corrections and the resulting action, if any.

If an individual has complaints or objections to the accuracy or completeness of information about him or her that originates with another agency, including information that is shared through the ISE, the Privacy Officer or legal counsel will notify the originating agency of the complaint or request for correction and coordinate with the originating agency to assist the individual with complaint and corrections procedures. A record will be kept of all such complaints and requests for corrections and the resulting action taken, if any.

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 IIFC; (b) allegedly resulted in harm to the complainant; and (c) is exempt from disclosure, the IIFC will inform the individual of the procedure for submitting (if needed) and resolving complaints or objections. Complaints should be directed to the IIFC Privacy Officer at the following e-mail address: iifc@iifc.in.gov. The IIFC 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, as permitted by law. If the information did not originate with the IIFC, IIFC will notify the originating agency in writing and, upon request, assist such agency to correct or purge any identified data/record deficiencies, subject to applicable records retention procedures, or to verify that the record is accurate. Any personal information originating with the IIFC will be reviewed and corrected in or deleted from IIFC data/records according to applicable records retention procedures if it is determined to be erroneous, include incorrectly merged information, or out of date. A record will be kept of all complaints and requests for corrections and the resulting action, if any.

An individual to whom information has been disclosed will be given reasons if requests for correction(s) are denied by the IIFC or originating agency, including ISE participating agencies, and be informed of any existing procedure for appeal.

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

I. SECURITY SAFEGUARDS

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

The IIFC will secure tips, leads, and ISE-SAR information in the same system that secures data rising to the level of reasonable suspicion under 28 CFR Part 23.

Queries made to the IIFC data applications will be logged into the data system identifying the user initiating the query.

The IIFC will utilize watch logs to maintain audit trails of requested and disseminated information.

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

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

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

The IIFC will notify an individual about whom personal information was or is reasonably believed to have been breached or obtained by an unauthorized person and access to which threatens physical, reputational, or financial harm to the person. The notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or any measures necessary to determine the scope of the release of information and, if necessary, to reasonably restore the integrity of any information system affected by this release.

The IIFC will immediately notify the originating agency from which the entity received personal information of a suspected or confirmed breach of such information.

J. INFORMATION RETENTION and DESTRUCTION

All identified person or organization information will be reviewed for record retention, as provided by 28 CFR Part 23, or a lesser period specified by state or local law.
IIFC personnel are required to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of tips and leads (including SAR information).

Center personnel will:

- Prior to allowing access to or dissemination of the information, ensure that attempts to validate

or refute the information have taken place and that the information has been assessed for sensitivity and confidence by subjecting it to an evaluation or screening process to determine its credibility and value and categorize the information as unsubstantiated or uncorroborated if attempts to validate or determine the reliability of the information have been unsuccessful. The center will use a standard reporting format and data collection codes for SAR information.

- Store the information using the same storage method used for data which rises to the level of reasonable suspicion, and which includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information.
- Allow access to or disseminate the information using the same (or a more restrictive) access or dissemination standard that is used for data that rises to the level of reasonable suspicion (for example, "need-to-know" and "right-to-know" access or dissemination for PII).
- Regularly provide access to or disseminate the information in response to an interagency inquiry for law enforcement, homeland security, or public safety and analytical purposes or provide an assessment of the information to any agency, entity, individual, or the public when credible information indicates potential imminent danger to life or property.
- Retain information for one year in order to work a SAR, tip or lead to determine its credibility and value or assign a "disposition" label so that a subsequently authorized user knows the status and purpose for the retention and will retain the information based on the retention period associated with the disposition label.
- Adhere to and follow the center's physical, administrative, and technical security measures to ensure the protection and security of tips, leads, and SAR information. Tips, leads, and SAR information will be secured in a system that is the same as or similar to the system that secures data that rises to the level of reasonable suspicion.

The IIFC 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, as well as information privacy, civil rights, and civil liberties. When information has no further value or meets the criteria for removal according to the IIFC's retention and destruction policy or according to applicable law, it will be purged, destroyed, and deleted or returned to the submitting source.

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

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

K. ACCOUNTABILITY and ENFORCEMENT

K.1 INFORMATION SYSTEM TRANSPARENCY

The IIFC will be open with the public in regard to information and intelligence collection practices. The IIFC privacy policy will be posted to the IIFC's website.

The IIFC's Privacy Officer will be responsible for responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s).

K.2 ACCOUNTABILITY

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

Requests for access for information for specific purposes will be referred to the Indiana State Police, Legal Division and/or Access to Public Records Act.

It is the intent of the Indiana Open Door Law that the official actions of public agencies should be conducted openly, unless otherwise expressly provided by statute, in order that citizens may be fully informed.

It is the intent of the Indiana Access to Public Records Act to permit citizens to have broad and easy access to public documents. By providing the public with the opportunity to review and copy public documents, the citizens have the opportunity to obtain information relating to government and to more fully participate in the government process. The IIFC will conduct business in accordance with the Indiana Access Public Records Act (IC 5-14-3) and will allow access to records and documents consistent with its requirements and exceptions. Inquiries about access to public records relating to IIFC data and documents should be addressed to the IIFC Administrator.

If a request for disclosure of a public record under the Indiana Access to Public Records Act is received by IIFC (including a request for ISE-SAR information posted to the shared space), such a public record may be disclosed to a member of the public only if the information is defined by law to be a public record or otherwise appropriate for release under the Indiana Access to Public Records Act and if such document is not exempt from disclosure by law. Such information may be disclosed only in accordance with applicable Indiana law.

The requesting individual to whom a record has been disclosed or withheld will be given a written reply which will delineate the records provided and the reasons for non-disclosure of any requested records which are denied by the IIFC. The individual will be informed of the procedure for filing a complaint with the Indiana Public Access Counselor or court if access to the record was denied.

If an individual has complaints or objections to the accuracy or completeness of ISE-SAR information about him or her that is alleged to be held by the IIFC, the IIFC, as appropriate, will inform the individual of the procedure for submitting complaints or requesting corrections. A record will be kept of all complaints and requests for corrections and the resulting action, if any.

The IIFC will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with their systems, in provisions of this policy and applicable law. This will include logging access of these systems and periodic auditing of these systems, so as to not establish a pattern of the audits. These audits will be mandated at least quarterly.

The IIFC's personnel or other authorized users shall report violations or suspected violations of agency/center policies relating to protected information to the IIFC Privacy Officer.

The IIFC will annually conduct an audit and inspection of the information contained in its criminal intelligence system. This auditor has the option of conducting a random audit, without announcement, at any time and without prior notice to the IIFC. This audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the center's criminal intelligence systems.

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

K.3 ENFORCEMENT

If IIFC personnel, personnel assigned to the IIFC from a participating agency, contractor, or any user of the IIFC is found to be in noncompliance with the provisions of this policy regarding the collection, use, retention, destruction, sharing, classification, or disclosure of information, the IIFC Administrator of the IIFC will:

- Suspend or discontinue access to information by the user;
- Suspend, demote, transfer, or terminate the person, as permitted by applicable personnel policies;
- Apply administrative actions or sanctions as provided by state police rules and regulations or as provided in agency/center personnel policies;
- If the user is from an agency external to the agency, request that the relevant agency, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions; or
- Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

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

APPENDIX A-TERMS and DEFINITIONS

28 C.F.R. Part 23—Section 28 Part 23 of the Code of Federal Regulations governs Criminal Intelligence Offices which receive federal funding to operate.

Access—Data access is being able to get to (usually having permission to use) particular data on a computer. Web access means having a connection to the World Wide Web through an access provider or an online service provider. Data access is usually specified as read-only and read/write access.

With regard to the ISE, access refers to the business rules, means, and processes by and through which ISE participants obtain terrorism-related information, to include homeland security information, terrorism information, and law enforcement information acquired in the first instance by another ISE participant.

Agency—Agency refers to the Indiana Intelligence Fusion Center and all agencies that access, contribute, and share information in the Indiana Intelligence Fusion Center's justice information system.

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

Audit trails are a fundamental part of computer security, used to trace (usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure, certificates, digital signatures, smart cards, biometric data, and a combination of usernames and passwords.

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

Center—Center refers to the Indiana Intelligence Fusion Center.

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

Civil Rights—The term "civil rights" refers to governments' role in ensuring that all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of

race, religion, gender, or other characteristics unrelated to the worth of the individual. Civil rights are, therefore, obligations imposed on government to promote equality. More specifically, they are the rights to personal liberty guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments and by acts of Congress.

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

Computer Security—The protection of information assets through the use of technology, processes, and training.

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

Data—Elements of information.

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

Fair Information Practice Principles—The Fair Information Practice Principles (FIPPs) are a set of eight principles rooted in the Privacy Act of 1974. Under the Homeland Security Act of 2002, DHS has implemented these as the basis for privacy compliance policies and procedures governing the use of personally identifiable information. Some of the individual principles may not apply in all instances of the integrated justice system.

Fusion Center—Defined in the ISE-SAR Functional Standard, Aug 2023 as "[a] collaborative effort of two or more Federal, State, local, tribal, or territorial (SLTT) government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity." (Source: Section 511 of the 9/11 Commission Act). State and major urban area fusion centers serve as focal points within the State and local environment for the receipt, analysis, gathering, and sharing of threat-related information between the federal government and SLTT and private sector partners.

Homeland Security Information—As defined in Section 892(f)(1) of the Homeland Security Act of 2002 and codified at 6 U.S.C. § 482(f)(1), homeland security information means any information possessed by a federal, state, or local agency that (a) relates to a threat of terrorist activity; (b) relates to the ability to prevent, interdict, or disrupt terrorist activity; (c) would improve the identification or investigation of a suspected terrorist or terrorist organization; or (d) would improve the response to a terrorist act.

IIFC Personnel—IIFC personnel may include state employees, state agency contractors or

subcontractors, and federal, state, or local agencies assigned to the IIFC.

Information—Information includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists. Information received by law enforcement agencies may be categorized in general areas, including, but not limited to, general data, tips and leads data, suspicious activity reports, criminal intelligence information, intelligence information, or investigatory records.

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

Information Sharing Environment (ISE)—In accordance with Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended, the ISE is a conceptual framework composed of the policies, procedures, and technologies linking the resources (people, systems, databases, and information) of SLTT agencies; federal agencies; and the private sector to facilitate terrorism-related information sharing, access, and collaboration.

Information Sharing Environment (ISE) Suspicious Activity Report (SAR) (ISE-SAR)—An ISE-SAR is a SAR that has been determined, pursuant to a two-step process established in the ISE-SAR Functional Standard, to have a potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism).

Intelligence (Criminal)—This means data which has been evaluated to determine that it: (i) is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity, and (ii) meets criminal intelligence system submission criteria.

Joint Terrorism Task Forces (JTTFs)—The Federal Bureau of Investigation's (FBI) JTTFs are interagency task forces designed to enhance communication, coordination, and cooperation in countering terrorist threats. They combine the resources, talents, skills, and knowledge of federal, state, territorial, tribal, and local law enforcement and homeland security agencies, as well as the Intelligence Community, into a single team that investigates and/or responds to terrorist threats. The JTTFs execute the FBI's lead federal agency responsibility for investigating terrorist acts or terrorist threats against the United States.

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

Law Enforcement Information—For purposes of the ISE, law enforcement information means any information obtained by or of interest to a law enforcement agency or official that is both (a) related to terrorism or the security of our homeland and (b) relevant to a law enforcement mission, including but not limited to information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of or response to criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected

of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of or response to criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance.

Lawful Permanent Resident—A foreign national who has been granted the privilege of permanently living and working in the United States.

Logs—See Audit Trail. Logs are a necessary part of an adequate security system because they are needed to ensure that data is properly tracked and that only authorized individuals are getting access to the system and the data.

Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)—The NSI establishes standardized processes and policies that provide the capability for federal, SLTT, campus, and railroad law enforcement and homeland security agencies to share timely, relevant ISE-SARs through a distributed information sharing system that protects privacy, civil rights, and civil liberties.

Nationwide SAR Initiative (NSI) SAR Data Repository (SDR)—The NSI SDR consists of a single data repository, built to respect and support originator control and local stewardship of data, which incorporates federal, state, and local retention policies. Within the SDR, hosted data enclaves extend this approach to information management and safeguarding practices by ensuring a separation of data across participating agencies.

Need to Know—This means the necessity to obtain or receive criminal intelligence information in the performance of official responsibilities as a law enforcement or criminal justice agency or authority.

Nonrepudiation—A technique used to ensure that someone performing an action on a computer cannot falsely deny that he or she performed that action. Nonrepudiation provides undeniable proof that a user took a specific action, such as transferring money, authorizing a purchase, or sending a message.

Non-validated Information—A tip or lead (including a SAR) received by the center that has been determined to be false or inaccurate or otherwise determined to not warrant additional action and/or maintenance.

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

Owning Agency/Organization—The organization that owns the target associated with the suspicious activity.

Permissions—Authorization to perform operations associated with a specific shared resource, such as a file, a directory, or a printer. Permissions must be granted by the system administrator to individual user accounts or administrative groups.

Personal Information—Information which can be used, either alone or in combination with other information, to identify individual subjects suspected of engaging in an activity or incident potentially related to terrorism.

Personally Identifiable Information (PII)—Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."

Preoperational Planning—As defined in ISE-SAR Functional Standard, Aug 2023, "preoperational planning describes activities associated with a known or particular planned criminal operation or with terrorist operations generally."

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

Privacy, Civil Rights, and Civil Liberties (P/CRCL) Policy—A printed, published statement that articulates the policy position of an organization on how it handles the PII that it maintains and uses in the normal course of business. The policy should include information relating to the processes of information collection, receipt, access, use, dissemination, retention, and purging. It is likely to be informed by the Fair Information Practice Principles (FIPPs). The purpose of the P/CRCL policy is to articulate that the center will adhere to those legal requirements and center policy determinations that enable collection, receipt, access, use, dissemination, retention, and purging of information to occur in a manner that protects personal privacy interests. A well-developed and implemented P/CRCL policy uses justice entity resources wisely and effectively; protects the center, the individual, and the public; and promotes public trust.

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

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

Privacy Protection—This is a process of maximizing the protection of privacy, civil rights, and civil

liberties when collecting and sharing information in the process of protecting public safety and public health.

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

For state, local, tribal, and territorial governments, protected information may include information about individuals and organizations that is subject to information privacy or other legal protections by law, including the U.S. Constitution; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 23; applicable state and tribal constitutions; and applicable state, local, tribal, and territorial laws, ordinances, and codes. Protection may be extended to other individuals and organizations by fusion center or other state, local, tribal, or territorial agency policy or regulation.

Public—Public includes:

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

Public does not include:

- Any employees of the center or participating entity.
- People or entities, private or governmental, who assist the center in the operation of the justice information system.
- Public agencies whose authority to access information gathered and retained by the center is specified in law.

Public Access—Relates to what information can be seen by the public; that is, information whose availability is not subject to privacy interests or rights.

Purge—A term that is commonly used to describe methods that render data unrecoverable in a storage space or to destroy data in a manner that it cannot be reconstituted. There are many different strategies and techniques for data purging, which is often contrasted with data deletion (e.g., made inaccessible except to system administrators or other privileged users).

Reasonably Indicative—This operational concept for documenting and sharing suspicious activity takes into account the circumstances in which that observation is made, which creates in the mind of the reasonable observer, including a law enforcement officer, an articulable concern that the behavior may indicate preoperational planning associated with terrorism or other criminal activity. It also takes into account the training and experience of a reasonable law enforcement officer, in cases in which an officer is the observer or documenter of the observed behavior reported to a law enforcement agency.

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

Redress—Internal procedures to address complaints from persons regarding protected information about them that is under the IIFC's control.

Retention—Refer to Storage.

Right to Know—This means the legal authority to obtain or receive criminal intelligence information pursuant to court order, statute or decisional law.

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

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

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

Shared Space—A networked data and information repository that is under the control of submitting agencies and which provides terrorism-related information, applications, and services to other ISE participants.

Sharing—Refers to the act of one ISE participant disseminating or giving homeland security information, terrorism information, or law enforcement information to another ISE participant.

Source Agency/Organization—Defined in the ISE-SAR Functional Standard, Aug 2023, source agency refers to the agency or entity that originates the SAR (examples include a local police department, a private security firm handling security for a power plant, and a security force at a military installation). The source organization will not change throughout the life of the SAR.

Storage—In a computer, storage is the place where data is held in an electromagnetic or optical form for access by a computer processor. There are two general usages: Storage is frequently used to mean the devices and data connected to the computer through input/output operations—that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-computer storage. This meaning is probably more common in the IT industry than meaning 2.

- In a more formal usage, storage has been divided into (1) primary storage, which holds data in memory (sometimes called random access memory or RAM) and other "built-in" devices such as the processor's L1 cache, and (2) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations.
- Primary storage is much faster to access than secondary storage because of the proximity of the storage to the processor or because of the nature of the storage devices. On the other hand, secondary storage can hold much more data than primary storage.
- With regard to the ISE, storage (or retention) refers to the storage and safeguarding of terrorism-related information, to include homeland security information, terrorism information, and law enforcement information relating to terrorism or the security of our homeland by both the originator of the information and any recipient of the information.

Submitting Agency/Organization—The organization that actuates the push of the ISE-SAR to the NSI community. The submitting organization and the source organization may be the same.

Suspicious Activity—Defined in the ISE-SAR Functional Standard, Aug 2023as "observed behavior reasonably indicative of preoperational planning associated with 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.

Suspicious Activity Report (SAR)—Defined in the ISE-SAR Functional Standard, Aug 2023, as "official documentation of observed behavior reasonably indicative of preoperational planning associated with terrorism or other criminal activity." Suspicious activity report (SAR) information offers a standardized means for feeding information repositories or data analysis tools. Patterns identified during SAR information analysis may be investigated in coordination with the reporting agency and, if applicable, a state or regional fusion center. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor is it designed to support interagency calls for service.

Terrorism Information—Consistent with Section 1016(a)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), all information relating to (a) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or materials support, or activities of foreign or international terrorist groups or individuals or of domestic groups or individuals involved in transnational terrorism, (b) threats posed by such groups or individuals to the United States, United

States persons, or United States interests or to those interests of other nations, (c) communications of or by such groups or individuals, or (d) other groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

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

§ 482(f)(1)); and (2) law enforcement information relating to terrorism or the security of our homeland). Such additional information includes intelligence information. Weapons of Mass Destruction (WMD) information as a fourth (third statutory) category of ISE information is not called for in P.L. 110-53. Rather, it amends the definition of terrorism information to include WMD information and then defines that term. WMD information probably should not technically be cited or referenced as a fourth category of information in the ISE.

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

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

Unvalidated information—A tip or lead (including a SAR) received by the center that has not yet been reviewed to determine further action or maintenance.

U.S. Person—Executive Order 12333 states that a "United States person" means a United States citizen, an alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.

User—An individual representing a participating agency who is authorized to access or receive and use a

center's information and intelligence databases and resources for lawful purposes. Validated Information—A tip or lead (including a SAR) that has been reviewed and, when appropriate, combined with other information or further vetted and is determined to warrant additional action, such as investigation or dissemination, and/or maintenance as per the applicable record retention policy.

THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY

THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY

THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY

THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY

THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY

APPENDIX B

Receipt of IIFC Privacy Policy
By IIFC and Non-IIFC Personnel

My signature below indicates that I have been provided a copy, have read it, and that I understand the Indiana Intelligence Fusion Center Privacy Policy. I understand that the Privacy Policy applies to me and that its violation may serve as a basis for disciplinary action, up to and including dismissal.

Signature: _____

Printed Name: _____

Date Signed: _____