THE IDAHO CRIMINAL INTELLIGENCE CENTER PRIVACY POLICY

1. PURPOSE

The mission of the Idaho Criminal Intelligence Center ([IC]^2) is to collect, store, analyze and disseminate information on crimes, including suspected offenses, to the law enforcement community and government officials regarding dangerous drugs, fraud, organized crime, terrorism and other criminal activity for the purpose of decision making, public safety and proactive law enforcement while ensuring the rights and privacy of citizens. This Privacy Policy is adopted to provide procedures for the protection of civil rights, civil liberties and the protection of personal privacy.

2. DEFINITIONS

Agency—The [IC]^2 and all agencies that access, contribute, and share information in the [IC]^2's justice information system.

Civil Rights—The term "civil rights" is used to imply that the state has a role in ensuring that all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of race, religion, gender or other characteristics unrelated to the worth of the individual. "Civil rights" encompasses "civil liberties," which 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 U.S. Constitution and all Amendments thereto. "Civil rights" also encompasses an individual's privacy interests in preventing the inappropriate collection, use, and release of personal information. Privacy interests include privacy of personal behavior, personal communications, and personal data. Other definitions of privacy include the capacity 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.

Code of Federal Regulations—The Code of Federal Regulations (CFR) is an annual codification of the general and permanent rules published in the Federal Register by the executive departments and agencies of the Federal Government.

Criminal Intelligence Information—Information deemed relevant to the identification of and the criminal activity engaged in by an individual who or organization that is reasonably suspected of involvement in criminal activity and meets criminal intelligence system submission criteria (See CFR Part 23.3). Criminal intelligence records are maintained in a criminal intelligence system per 28 CFR Part 23.

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 that may be available only to certain people for certain purposes but is not available to everyone.

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

Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.5.5—is defined by the Office of the Director of National Intelligence website located at: https://www.dni.gov/files/ISE/documents/DocumentLibrary/SAR/SAR_FS_1.5.5_IssuedFeb2015.pdf

Information Sharing Environment (ISE) Suspicious Activity Report (SAR) (ISE-SAR)—A SAR that has been determined, pursuant to a two-step process established in the Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.5.5, to have a potential terrorism nexus (for example, to be reasonably indicative of criminal activity associated with terrorism).

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

Originating Agency—The agency or organizational entity that documents information or data, including source agencies that document SAR or ISE-SAR information that is collected by an agency.

Participating Agency—An organizational entity that is authorized to access or receive and use [IC][2] information and/or intelligence databases and resources for lawful purposes through its authorized individual users.

Personal Data—Refers to any information that relates to an identifiable individual or data subject. *See also* Personally Identifiable Information (PII).

Personal Information—Information that can be used, either alone or in combination with other information, to identify individual subjects suspected of engaging in criminal activity, including terrorism. *See also* Personally Identifiable Information (PII).

Personally Identifiable Information (PII)—One or more pieces of information that, when considered together or in the context of how the information is presented or gathered, are sufficient to specify a unique individual. The pieces of information can be:

> Personal characteristics (for example height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation, place of birth, mother's maiden name, distinguishing features, and biometrics information, such as fingerprints, DNA, and retinal scans).

A unique set of numbers or characters assigned to a specific individual (for example name, address, phone number, social security number, e-mail address, driver's license number, financial account or credit card number and associated PIN number, Integrated Automated Fingerprint Identification System (IAFIS) identifier, or booking or detention system number).

Description(s) of event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records).

Description(s) of location(s) or place(s) (for example Geographic Information Systems (GIS) locations, electronic bracelet monitoring information, etc.).

Protected Information —Includes personal data (Personally Identifiable Information) about individuals that is subject to information privacy and other legal protections by law, including the U.S. Constitution and the Idaho 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, and tribal laws and ordinances. Protection may also be extended to organizations by $[IC]^2$ policy or state, local, or tribal law.

Public—Public includes:

1. Any person and any for-profit or nonprofit entity, organization, or association;
2. Any governmental entity for which there is no existing specific law authorizing access to the agency's/$[IC]^2$'s information;
3. Media organizations;
4. Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the agency.

Public does not include:

1. Employees of the agency;
2. People or entities, private or governmental, who assist the agency or $[IC]^2$ in the operation of the justice information system;
3. Public agencies whose authority to access information gathered and retained by the agency or $[IC]^2$ is specified by law.

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

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

Source Agency —Source agency refers to the agency or organizational entity that originates SAR and/or ISE-SAR information.

Suspicious Activity —Defined in the ISE-SAR FS 1.5.5 as "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, cyber attacks, testing of security, etc.

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 into 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.

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), 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 to being extremely valuable. This also depends on the availability of time and resources to analyze the tip or lead to determine its meaning and value.

United States Code (USC) — The United States Code (USC) is the codification by subject matter of the general and permanent laws of the United States. It is divided by broad subjects into 53 titles and published by the Office of the Law Revision Counsel of the U.S. House of Representatives. Stated most simply, the USC are federal statutes/laws enacted by the U.S. Congress.

3. POLICY APPLICABILITY AND LEGAL COMPLIANCE

A. All $[IC]^2$ personnel and agencies receiving or submitting information to the $[IC]^2$ and participating personnel will comply with this Privacy Policy, which is in compliance with the United States Constitution, the Idaho Constitution, the Criminal Intelligence Systems Operating Policies (28 CFR Part 23), the Bank Secrecy Act (31 USC 5311), the Idaho Public Records Act, specifically IDAHO CODE § 74-124 (exemption from disclosure of investigatory records compiled for law enforcement purposes by a law enforcement agency), IDAHO CODE § 74-104(1) (exemption from disclosure of any

public record exempt from disclosure by federal or state law or federal regulations to the extent specifically provided for by such law or regulation), IDAHO CODE § 74-105(1) (exemption from disclosure of investigatory records of a law enforcement agency, as defined in IDAHO CODE § 74-101(7), under the conditions set forth in IDAHO CODE § 74-124), and all other relevant civil rights, constitutional and statutory laws (including but not limited to those cited in Appendix A of this Privacy Policy) that pertain to the information the [IC]^2 collects, receives, maintains, archives, accesses, or discloses. This Policy applies to information the [IC]^2 gathers or collects, receives, maintains, stores, accesses, discloses, or disseminates to [IC]^2 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.

B. If an authorized user does not comply with the provisions of this Policy regarding the collection, use, retention, destruction, sharing, classification or disclosure of information, the [IC]^2 Supervisor will:
    a. Suspend or discontinue user access to the information;
    b. Discipline the authorized user as permitted by applicable personnel policies up to and including dismissal;
    c. If the user is from an agency external to the [IC]^2, the [IC]^2 Supervisor will report the misuse to the relevant agency, organization, contractor or service provider employing the offending user; and/or
    d. Refer the matter to appropriate authorities for criminal prosecution, as applicable.

C. The [IC]^2 will provide training regarding this Policy as part of new employee training and to participating personnel as part of the new intelligence system user training. This training will include implementation of and adherence to the [IC]^2 Privacy Policy as it applies to any and all information collected, retained or shared by the [IC]^2. This training will be required for:
    a. All personnel assigned to [IC]^2;
    b. Personnel providing information technology services to the [IC]^2;
    c. Staff in other public agencies and private contractors providing services to the agency;
    d. Users who apply for access to [IC]^2 information.

D. The [IC]^2 will provide special training regarding the [IC]^2's requirements and policies for collection, use, and disclosure of protected information to personnel authorized to share protected information through the Information Sharing Environment (ISE).

E. The Privacy Policy training program will cover:
    a. Purposes of [IC]^2 Privacy Policy.

b. Substance and intent of the provisions of this Policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the [IC]^2.
c. Originating and participating agency responsibilities and obligations under applicable law and policy.
d. How to implement this Policy in the day-to-day work of the user, regardless of the role of the user.
e. The impact of improper activities associated with infractions within or through the agency.
f. Mechanisms for reporting violations of [IC]^2 Privacy Policy and procedures.
g. The nature and possible penalties for Policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.

F. The [IC]^2 has adopted internal operating policies that are in compliance with applicable laws protecting civil rights, including, but not limited to: the United States Constitution, the Idaho Constitution, the Criminal Intelligence Systems Operating Policies (28 CFR Part 23), the Bank Secrecy Act (31 USC 5311), and the Idaho Public Records Act, specifically IDAHO CODE §§ 74-124, 74-104(1), and 74-105(1).

4. GOVERNANCE AND OVERSIGHT

A. The Idaho State Police will house [IC]^2 and the [IC]^2 Supervisor has the primary responsibility for the day to day operation of [IC]^2 including:
    a. Coordination of [IC]^2 personnel regarding [IC]^2 functions, such as:
        i. Collection, receipt, retention, and evaluation of information and
        ii. Analysis, destruction, sharing or disclosure of such information.

B. Pursuant to the [IC]^2 Memorandum of Understanding, the Governance Board for [IC]^2 shall consist of one command staff member from each of the agencies who provide staff to [IC]^2, which shall include the Federal Bureau of Investigation (FBI) and the Office of the Attorney General for the State of Idaho.
C. The Governance Board shall adopt standards and procedures for the operation of this section.
    a. The Governance Board will recommend the approval or denial of an agency's participation in the [IC]^2. The Governance Board will recommend the suspension of a participant agency for due cause and recommend, if appropriate, the reinstatement of a suspended participant agency.
    b. The Governance Board may periodically inspect records relating to dissemination of information to determine whether [IC]^2 and its authorized users are in compliance with this Privacy Policy, and make recommendations, as they deem appropriate, to [IC]^2 management.

c. The Governance Board shall review and be responsible for the approval of all policy and procedures of the [IC]^2, including this Privacy Policy, which will be reviewed and updated on an annual basis.
d. This Policy is not protected under the provisions of governing state and federal law and will be disclosed to the public upon request to the [IC]^2 Supervisor or Governance Board and will be posted on the [IC]^2 webpage at https://www.isp.idaho.gov/icic/ and via the main Idaho State Police website at https://www.isp.idaho.gov/.

5. INFORMATION SECURITY AND SAFEGUARDS

A. The [IC]^2 will operate in a secure environment protecting the facility from external intrusion. The [IC]^2 utilizes secure internal and external safeguards against network intrusions. Access to [IC]^2 databases from outside the facility will only be allowed over secure networks.
   a. The [IC]^2 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.
   b. Access to, analysis and dissemination of [IC]^2 information will only be granted to [IC]^2 personnel whose positions and job duties require such access and who have successfully completed background checks and appropriate security clearances, if applicable, and been selected, approved, and trained accordingly.
   c. Credentialed, role-based access criteria will be used by the [IC]^2, as appropriate, to control:
      i. The information to which a particular group or class of users can have access based on the group or class.
      ii. The information a class of users can add, change, delete, or print.
      iii. To whom, individually, the information can be disclosed and under what circumstances.
   d. The [IC]^2 only maintains criminal intelligence information that will be handled in accordance with 28 CFR Part 23 and made available to participating agencies and authorized users on a "need to know" and "right to know" basis.
   e. The [IC]^2 will maintain records of requested information that is accessed and disseminated.
   f. In order to prevent inadvertent public disclosure, risk and vulnerability assessments will not be stored with publicly available data.
   g. The [IC]^2 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 the physical well-being, reputation, or finances of the person. The notice will be made promptly and without unreasonable delay following discovery 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.

B. The [IC]^2 Director shall designate trained and qualified members of the [IC]^2 to serve as the Privacy and Security Officers.
    a. The [IC]^2's Privacy Committee, a subcommittee of the [IC]^2 Governance Board, is guided by a trained Privacy Officer who is appointed by the [IC]^2 Director. The Privacy Officer receives reports regarding alleged errors and violations of the provisions of this Policy, receives and coordinates complaint resolution under the [IC]^2's redress policy, and serves as the liaison for the Information Sharing Environment (ISE), ensuring that privacy protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy enhancing technologies. The Privacy Officer can be contacted at the following address: 700 S. Stratford Dr., Meridian, Idaho 83642.

C. The [IC]^2 Director ensures that enforcement procedures and sanctions outlined in section 3, Policy Applicability and Legal Compliance, are adequate and enforced.

6. INFORMATION GATHERING AND ACQUISITION

A. The [IC]^2 and contributing agencies will adhere to the Criminal Intelligence Guidelines established under the U.S. Department of Justice (DOJ) National Criminal Intelligence Sharing Plan (NCISP); 28 CFR Part 23 regarding criminal intelligence information; the Organization for Economic Cooperation and Development (OECD) Fair Information Principles (under certain circumstances, there may be exceptions to the Fair Information Principles, based, for example, on authorities paralleling those provided in the federal Privacy Act); the U.S. and Idaho Constitutions; state and local law as referenced in IDAHO CODE (see Appendix A); or [IC]^2 policy.

B. The [IC]^2 will use the least intrusive techniques possible in the particular circumstance to gather information it is authorized to seek or retain.

C. Agencies participating in the [IC]^2 or providing information to the [IC]^2 are subject to the laws and rules governing those individual agencies, as well as by applicable federal, state and tribal laws identified in section 3.A. In the event of a conflict, applicable federal, state and tribal laws identified in section 3.A and this Privacy Policy will control and take precedence.

D. The [IC]^2 will contract only with commercial database entities that provide an assurance that they gather Personally Identifiable Information in compliance with local, state, tribal, territorial and federal laws, and information that is not based on misleading information collection practices.

E. The [IC]^2 will not directly or indirectly receive, seek, accept, or retain information from an individual or nongovernmental information provider who may or may not receive a fee or benefit for providing the information if the [IC]^2 knows or has reason to believe that the individual or information provider is legally prohibited from obtaining or disclosing the information or used a source that gathered the information by prohibited means.

F. The [IC]^2 will seek or retain information that:
    a. Is based on a possible threat to public safety or the enforcement of the criminal law; or
    b. Is based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal conduct or activity, including terrorist activity, that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal conduct or activity, including terrorist activity; or
    c. Is relevant to the investigation and prosecution of suspected criminal incidents, including terrorist activity, the resulting justice system response, the enforcement of sanctions, orders, or sentences, or the prevention of crime; or
        i. Is useful in crime analysis or in the administration of criminal justice and public safety (including topical searches); and
        ii. The source of the information is reliable and verifiable or limitations on the quality of the information are identified; and
        iii. The information was collected in a fair and lawful manner, with the knowledge and consent of the individual, if applicable.
    d. The [IC]^2 may retain protected information that is based on a level of suspicion that is less than "reasonable suspicion," such as tips and leads or suspicious activity report (SAR) information, subject to the policies and procedures specified in this Policy.

G. All information (defined and identified in this section) acquired or received by the [IC]^2 is analyzed according to priorities and needs and will be analyzed only to:
    a. Further crime prevention, including the prevention of terrorist activity, law enforcement, public safety, force deployment, or prosecution objectives and priorities established by the [IC]^2, and/or
    b. Provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal and/or terrorist activities.

H. The [IC]^2 Privacy Officer shall be responsible for receiving and responding to inquiries and complaints about civil rights protections in the information system. The [IC]^2 Privacy Officer can be contacted at the following address: 700 S. Stratford Dr., Meridian, Idaho 83642.

I. The [IC]^2 will not seek or retain and information originating agencies will agree not to submit information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their race, ethnicities, citizenship, places of origin, ages, disabilities, genders, or sexual orientations.

7. INFORMATION QUALITY ASSURANCE

A. The [IC]^2 will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources of information (including whether it meets 28 CFR Part 23), that is accurate, current, and complete, including the relevant context in which it was sought or received and will be merged with other information about the same individual or organizations only when the applicable standards for information gathering and acquisition (identified in section 6 of this Privacy Policy) have been met. The [IC]^2 personnel will, upon receipt of information, assess and categorize the information to determine or review its nature, usability, and quality.

B. At the time of retention in the system, the information will be labeled regarding its level of quality, accuracy, completeness, currency, and confidence (whether it is verifiable and reliable).

C. The [IC]^2 will investigate, in a timely manner, alleged errors and deficiencies, and correct or delete, and refrain from using protected information found to be erroneous or deficient.

D. The labeling of retained information will be re-evaluated when new information is gathered that has an impact on the [IC]^2's confidence in the validity or reliability of retained information.

E. The [IC]^2 will conduct periodic data quality reviews of information it originates and will make every reasonable effort to ensure that information will be corrected, deleted from the system, or not used when the [IC]^2 identifies information that is erroneous, misleading, obsolete or otherwise unreliable, the [IC]^2 did not have the authority to gather the information or to provide the information to any other agency, or the [IC]^2 used prohibited means to gather information, except when the [IC]^2's information source did not act as the agent of the [IC]^2 in gathering the information.

F. Federal, state, local and tribal agencies, including agencies participating in the ISE, are responsible for the quality and accuracy of the data accessed by or shared with the [IC]^2. Originating agencies providing data will be advised, by written electronic notification (such as email), if data from that agency is found to be inaccurate, incomplete, out of date, or unverifiable.

G. The [IC]^2 will use written or documented electronic notification to inform recipient agencies when information previously provided by the [IC]^2 is deleted or changed by the

[IC]^2 because it is erroneous or deficient such that the rights of the individual may be affected (for example, if it is determined to be inaccurate or includes incorrectly merged information).

H. The [IC]^2 applies labels to agency-originated information or ensures that the originating agency has applied labels to indicate to the accessing authorized user that:
    a. The information is protected information as defined in section 2 of this Privacy Policy and, to the extent expressly provided in this Policy, includes organizational entities.
    b. The information is subject to 28 CFR Part 23 or to federal, state, or local law restricting access, use, or disclosure.

I. [IC]^2 personnel are required to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of tips and leads and suspicious activity report (SAR) information. [IC]^2 personnel are required to do the following:
    a. 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 [IC]^2 will use a standard reporting format and data collection codes for SAR information.
    b. 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.
    c. Allow access to or disseminate the information using the same or 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 Personally Identifiable Information).
    d. 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.
    e. Retain information for 180 days in order to work a not yet validated tip, lead, or SAR information to determine its credibility and value or assign a “disposition” label (for example, undetermined or unresolved, cleared or unfounded, verified, or under active investigation) 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.

f. Adhere to and follow the [IC]^2'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.
g. Provide for human review and vetting to ensure that information is both legally gathered and, where applicable, determined to have a potential terrorism nexus. Law enforcement officers and appropriate [IC]^2 and participating agency staff will be trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism.
h. The [IC]^2'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 will not be intentionally or inadvertently gathered, documented, processed, and shared.
i. The [IC]^2 adheres to the current version of the Information Sharing Environment Functional Standard Suspicious Activity Reporting (ISE FS-SAR 1.5.5) 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 FS-SAR 1.5.5 for suspicious activity potentially related to terrorism.
j. The [IC]^2 incorporates the gathering, processing, reporting, analyzing, and sharing of terrorism-related SARs 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 civil rights.
k. The [IC]^2 will secure tips, leads, and 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.

8. INFORMATION RETENTION AND DESTRUCTION

A. When participating agencies contribute information, they will assess the information to identify the criminal activity the information refers to, the nature of the source, the reliability of the source, and the validity of the content.

B. When the information is received, it will be reviewed by [IC]^2 analysts or [IC]^2 Supervisor for compliance with 28 CFR Part 23. Information that is noncompliant with these standards will be purged. Information that is compliant with these standards will be placed in the [IC]^2 intelligence database.

C. The [IC]^2 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 has assigned categories to the information) to reflect the assessment, such as:

a. Whether the information consists of tips and leads data, suspicious activity reports (SAR), criminal history, intelligence information, case records, conditions of supervision, case progress, or other information category.
b. The nature of the source as it affects veracity (for example, anonymous tip, trained interviewer or investigator, public record, private sector).
c. The reliability of the source (for example, reliable, usually reliable, unreliable, unknown).
d. The validity of the content (for example, confirmed, probable, doubtful, cannot be judged).

D. All retained information will be labeled by record, data set or system of records pursuant to applicable limitations on access and sensitivity of disclosure in order to:

a. Protect confidential sources, techniques and methods;
b. Protect and preserve pending criminal investigations;
c. Protect an individual's civil rights; and
d. Provide legally required protection based on the individual's status as a juvenile, victim, resident of or participant in a substance abuse treatment program or mental health treatment program, or resident of a domestic abuse shelter.

E. All applicable information will be reviewed for record retention at least every five (5) years, as provided by 28 CFR Part 23.

a. When information has no further value or meets the criteria for removal according to according to 28 CFR Part 23, it will be destroyed or returned to the submitting agency.
b. The $[IC]^2$ will delete information or return it to the submitting source, unless it is validated, every five (5) years, as provided in 28 CFR Part 23.
c. Permission to destroy or return information or records will be presumed as established by participating agreement if the applicable information is not validated within the specified time period.
d. Notification of proposed destruction or return of records will not be provided to the submitting agency.
e. A record of information reviewed for retention will be maintained by the $[IC]^2$.
f. A record of the date for review for retention will be maintained by the $[IC]^2$ and no notice will be given to the submitter prior to the required review and validation or purge date.

F. The classification of existing information will be re-evaluated when new information is added or existing information is changed that affects access or disclosure limitations.

G. The $[IC]^2$ requires certain basic descriptive information to be entered and electronically associated with data or content that is to be accessed, used, and disclosed, including:

a. The name of the originating agency and investigator; and
b. The date the information was collected and the date its accuracy was last verified.

H. The [IC]^2 will label information that will be accessed and disseminated to notify the accessing authorized user that the information is subject to state and federal laws restricting access, use or disclosure, including terrorism-related information shared through the ISE. The [IC]^2 will apply specific labels and descriptive metadata to clearly indicate all legal restrictions on information sharing based on information sensitivity or classification.

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

J. If the matching requirements are not fully met but there is an identified partial match, the information may be associated by the [IC]^2 if accompanied by a clear statement that it has not been adequately established that the information relates to the same individual or organization.

9. INFORMATION SHARING AND DISCLOSURE

A. Access to or disclosure of records retained by the [IC]^2 will only be provided to persons within the [IC]^2 or other governmental agencies who are authorized to access, analyze and disseminate and have a legitimate law enforcement, public safety or criminal justice purpose. Additionally, such disclosure or access shall only be granted for the performance of official duties in accordance with law and procedures applicable to the agency for which the person is employed. An audit trail will be kept of access by or dissemination to such persons. An audit trail of access by or dissemination to such persons will be maintained by [IC]^2.

B. Information gathered and records retained by the [IC]^2 will not be:
   a. Sold, published, exchanged or disclosed for commercial purposes;
   b. Disclosed or published without prior notice and/or permission of the contributing agency; or
   c. Disseminated to unauthorized persons.

C. Participating agencies may not disseminate information received from [IC]^2 without approval from the originating agency.

D. Information gathered and records retained by the [IC]^2 may be accessed or disclosed to a member of the public only if the information is not exempted by the Idaho Public Records Act and is otherwise appropriate for release. Such information may only be

disclosed in accordance with applicable law and an audit trail will be kept of all requests for information and what information is released to the public.

E. Information gathered or collected and records retained by the [IC]^2 may be accessed or disseminated for specific purposes upon request by persons authorized by law to have such access and only for those uses and purposes specified in the law. An audit trail sufficient to allow the identification of each individual who requested, accessed, or received information retained by the [IC]^2; the nature of the information requested, accessed, or received; and the specific purpose will be kept for a minimum of three years after the audit record is closed, terminated, completed, expired, settled or from its last date of contact by the [IC]^2. *See* Idaho Department of Administration Records Retention Schedule, Law Enforcement Records, Series # SG 1601 Activity Reports, Law Enforcement, (https://history.idaho.gov/wp-content/uploads/2018/08/Law_Enforcement_Records_Book_0.pdf).

F. Information about an individual about whom information has been gathered will only be disclosed under the provisions of IDAHO CODE § 74-113, upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information. The [IC]^2'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. The existence, content, and source of the information will not be made available by the [IC]^2 to an individual when:
    a. Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution. IDAHO CODE §§ 74-124 and 74-105(1).
    b. Disclosure would endanger the health or safety of an individual, organization, or community. IDAHO CODE §§ 74-124 and 74-105(1).
    c. The information is in a criminal intelligence information system subject to 28 CFR Part 23. *See* 28 CFR § 23.20(e).
    d. Information that meets the definition of "classified information" as that term is defined in the National Security Act, Public Law 235 Section 606 and in accordance with any/all related Executive Orders currently effective; *see also* IDAHO CODE § 74-104(1).
    e. Other authorized basis for denial, for example pursuant to Idaho Public Records Act, Title 74, Chapter 1, IDAHO CODE, or
    f. The information does not originate with the [IC]^2, in which case the [IC]^2 will coordinate with the source agency in responding to the request.

G. There are several categories of records that will ordinarily not be provided to the public:
    a. Criminal investigative information and criminal intelligence information. IDAHO CODE §§ 74-124, 74-104(1), and 74-105(1). However, certain law enforcement

records must be made available for inspection and copying under IDAHO CODE 74-124(3).

b. Other information that is protected from disclosure under the Idaho Public Records Act, Title 74, Chapter 1, IDAHO CODE.

H. The [IC]^2 shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive such information.

I. The [IC]^2 will comply with court orders for dissemination of information. Records of all such court orders and information disclosed pursuant to those court orders shall be kept.

J. An assessment of information gathered and retained by the [IC]^2 may be released to a government official or to any individual, when necessary, to avoid imminent danger to life or property pursuant to 28 CFR Part 23 § 23.20(f)(2). Records retained by the [IC]^2 may be accessed by or disseminated to those responsible for public protection, public safety, or public health only for public protection, public safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures. An audit trail sufficient to allow the identification of each individual who accessed or received information retained by the [IC]^2 and the nature of the information accessed will be kept by the [IC]^2.

10. COMPLAINTS AND CORRECTIONS

A. If an individual requests correction of information originating with the [IC]^2 that has been disclosed, the [IC]^2 Privacy Officer or designee will inform the individual of the procedure for requesting and considering requested corrections under IDAHO CODE § 74-113, including appeal rights if requests are denied in whole or in part. A record will be kept of all requests for corrections and the resulting action, if any, for 180 calendar days from the date of mailing of the notice of denial or partial denial of request for correction of information by the [IC]^2. IDAHO CODE § 74-115.

B. If an individual has a complaint with regard to the accuracy or completeness of protected information that:

a. Is exempt from disclosure,
b. Has been or may be shared through the ISE,
c. Is held by the [IC]^2 and
d. Allegedly has resulted in demonstrable harm to the complainant,

the [IC]^2 will inform the individual of the procedure for submitting and resolving such complaints. Complaints will be received by the [IC]^2 Privacy Officer or [IC]^2 Supervisor at the following address: 700 S. Stratford Dr., Meridian, Idaho 83642. The [IC]^2 Privacy Officer or [IC]^2 Supervisor will acknowledge the complaint and state that it will be reviewed but will not confirm the existence or nonexistence of the information to the complainant unless otherwise required by law. If the information did not originate with

the [IC]^2, the [IC]^2 Privacy Officer or [IC]^2 Supervisor will notify the originating agency in writing or electronically within 10 days and, upon request, assist such agency to correct any identified data/record deficiencies, purge the information, or verify that the record is accurate. All information held by the [IC]^2 that is the subject of a complaint will be reviewed within 30 days and confirmed or corrected/purged if determined to be inaccurate, incomplete, to include incorrectly merged information, or to be out of date. If there is no resolution within 30 days, the [IC]^2 will not share the information until the complaint has been resolved.

C. A record will be kept by the [IC]^2 of all complaints and the resulting action taken in response to the complaint.

D. The individual who has requested disclosure or to whom information has been disclosed will be given reasons if disclosure or requests for corrections are denied by the [IC]^2 or the originating agency. The individual will also be informed of the procedure for appeal when the [IC]^2 or originating agency has cited an exemption for the type of information requested or has declined to correct challenged information to the satisfaction of the individual to whom the information relates. Ref. section 10.A. above.

11. SYSTEMS ACCOUNTABILITY

A. Queries made to the [IC]^2 data applications will be logged into the data system identifying the user initiating the query.

B. The [IC]^2 will maintain an audit trail of accessed, requested, or disseminated information. An audit trail will be kept for a minimum of three years after the audit record is closed, terminated, completed, expired, settled or from its last date of contact by the [IC]^2. *See* Idaho Department of Administration Records Retention Schedule, Law Enforcement Records, Series # SG 1601, Activity Reports, Law Enforcement, (https://history.idaho.gov/wp-content/uploads/2018/08/Law_Enforcement_Records_Book_0.pdf).

C. The [IC]^2 will provide an electronic copy of this Policy to all persons who have access to the intelligence system and will require written acknowledgement of receipt of this Policy and agreement to compliance with the provisions of this Policy.

D. The [IC]^2 will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of persons who have access to the intelligence system with the provisions of this Policy and applicable law. This will include logging access of these systems and periodic auditing of these systems.

E. The [IC]^2 reserves the right to restrict the qualifications and number of personnel having access to [IC]^2 information.

F. The [IC]^2 will conduct an annual audit and inspection of the information and intelligence contained in its information system(s). The audit will be conducted by the [IC]^2 Privacy and Security Committee which is established by the [IC]^2 Governance Board. This committee has the option of conducting a random audit, without announcement, at any time and without prior notice to staff of the [IC]^2. The audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the [IC]^2's information and intelligence system(s).

G. The [IC]^2 personnel or other authorized users will report violations or suspected violations of [IC]^2 policies relating to protected information to the [IC]^2 Director, Supervisor, or Privacy Officer.

H. The [IC]^2 Director, Supervisor, and Privacy Officer, in conjunction with the Privacy Committee of the Governance Board, will annually review and update the provisions protecting civil rights contained within this Policy and make appropriate modifications in response to changes in applicable law, changes in technology, and changes in the purpose and use of the information systems.

Appendix A

Laws Relevant to Seeking, Retaining, and Disseminating Justice Information

State Laws:

IDAHO CODE § 74-124 (exemption from disclosure of investigatory records compiled for law enforcement purposes by a law enforcement agency).

IDAHO CODE § 74-104(1) (any public record exempt from disclosure by federal or state law or federal regulations to the extent specifically provided for by such law or regulation).

IDAHO CODE § 74-105(1) (Investigatory records of a law enforcement agency, as defined in IDAHO CODE § 74-101(7), under the conditions set forth in IDAHO CODE § 74-124).

Idaho Department of Administration Records Retention Schedule, Law Enforcement Records, Series # SG1601, Activity Reports, Law Enforcement.

Idaho Public Records Act, Title 74, Chapter 1, IDAHO CODE.

Federal Laws:

Brady Handgun Violence Prevention Act, 18 U.S.C. §§ 921, 922, 924, and 925A.

Computer Matching and Privacy Act of 1988, 5 U.S.C. § 552a(a), *see also* Office of Management and Budget, Memorandum M-01-05, "Guidance on Interagency Sharing of Personal Data–Protecting Personal Privacy," December 20, 2000.

Confidentiality of Identifiable Research and Statistical Information, 28 CFR Part 22.

Crime Identification Technology, 42 U.S.C. § 14601 (Transferred to 34 U.S.C. § 40301).

Exchange of Criminal History Records for Noncriminal Justice Purposes, 34 U.S.C. § 40311 (formerly 42 U.S.C. § 14611).

Criminal Intelligence Systems Operating Policies, 28 CFR Part 23.

Criminal Justice Information Systems, 28 CFR Part 20.

Disposal of Consumer Report Information and Records, 16 CFR Part 682.

Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510–2522, 2701–2709, 3121–3125; Public Law 99-508.

Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681.

Federal Civil Rights laws, 42 U.S.C. § 1983.

Freedom of Information Act (FOIA), 5 U.S.C. § 552.

HIPAA, Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 201 et seq; Public Law 104-191.

HIPAA, Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164.

Indian Civil Rights Act of 1968 (ICRA), 25 U.S.C. §§ 1301 - 1304.

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

National Child Protection Act of 1993, Public Law 103-209 (December 20, 1993), 107 Stat. 2490; 34 USC §§ 40101 – 40104.

National Crime Prevention and Privacy Compact of 1998, 42 U.S.C. §§ 14611 to 14616.

Privacy Act of 1974, 5 U.S.C. § 552a.

Privacy of Consumer Financial Information, 16 CFR Part 313.

Protection of Human Subjects, 28 CFR Part 46.

Standards for Safeguarding Customer Information, 16 CFR Part 314.

Sarbanes-Oxley Act of 2002, 15 U.S.C., Chapter 98, § 7201 et seq.

U.S. Constitution, including the Bill of Rights.

USA PATRIOT Act, 8 USC §§ 1226a, 1379; 15 USC § 1681v; 18 USC §§ 175b, 1993, 2339, 2712; 22 USC § 262p–4r, 7210, 7211; 31 USC §§ 310, 311, 5318A, 5319; 34 USC §§ 10286, 30102; 42 USC § 5195c; 49 USC § 5103a; 50 USC §§ 1861, 1862, 3040, 3365.