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

Computer-Aided Dispatch (CAD)—A system that assists law enforcement agencies' dispatchers with documenting calls for service from the public or other law enforcement agencies. CAD systems contain the raw data dispatchers enter to document and provide information to responding officers to enhance officer/public safety and dictate proper police response to a given call for assistance.

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), also known as "Federal Administrative Rules," 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

28 CFR Part 23.3). Criminal intelligence records are maintained in a criminal intelligence system pursuant to 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, and can occupy one or more of, 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 and housed at the Department of Homeland Security website as a downloadable document:

https://www.dhs.gov/sites/default/files/publications/15_0223_NSI_ISE-Functional-Standard-SAR.pdf

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

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 $[IC]^2$.
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 (as defined above), 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 records of incidents that omit indication of a criminal offense, criminal history records, or CAD (as defined above) 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. Its value and meaning are also dependent on the availability of time and resources to analyze the tip or lead.

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 [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 (12 USC §§ 1951 – 1959, see also 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 [IC]^2 collects, receives, maintains, archives, accesses, or discloses. This Policy applies to information [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. [IC]^2 provides special training regarding [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).

C. [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 (12 USC §§ 1951 – 1959, see also 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 houses [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 [IC]^2 Governance Board shall consist of one command staff member (including the Federal Bureau of Investigation (FBI) and the Office of the Attorney General for the State of Idaho) and from each of the agencies who provide staff to [IC]^2.

C. The Governance Board has adopted standards and procedures for the operation of this section.
    a. The Governance Board holds the authority to approve, suspend, reinstate, or deny an agency's participation with [IC]^2 for due cause, if appropriate.
    b. The Governance Board may periodically inspect [IC]^2 records relating to dissemination of information to determine whether [IC]^2 and its authorized users are in compliance with this Privacy Policy/applicable law, and make recommendations, as they deem appropriate, to [IC]^2 management.
    c. The Governance Board is responsible for the review and approval of all policies and procedures of [IC]^2, including this Privacy Policy. This Privacy Policy 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. [IC]^2 operates in a secure environment protecting the facility from external intrusion. [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. [IC]^2 will store information in a manner such that it cannot be added to, modified, accessed, destroyed, or purged except by authorized personnel.
    b. Analysis, dissemination, and access to [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, obtained appropriate security clearances, and, if applicable, been selected, approved, and trained accordingly.
    c. [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.

d. [IC]^2 will maintain records of requested information that is accessed and disseminated.
e. [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.

B. The [IC]^2 Director shall designate trained and qualified members of the [IC]^2 to serve as the Privacy and Security Officers. [IC]^2 Governance Board approves a board of oversight and inspection to facilitate the Governance and Oversight section (4.C.b.) of this Policy.
   a. [IC]^2's Governance Board will approve a trained Privacy Officer who is appointed by the [IC]^2 Director.
   b. 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. [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 (as defined above); 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. [IC]^2 uses the least intrusive techniques possible in the particular circumstance to gather information it is authorized to seek or retain.

C. Agencies participating in [IC]^2 or providing information to [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. [IC]^2 contracts 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. [IC]^2 does not directly or indirectly receive, seek, accept, or retain information from an individual or non-governmental 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. [IC]^2 seeks/retains 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. [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. Information received by [IC]^2 is analyzed with an eye towards fulfilling the mission of:
    a. Crime prevention, including the prevention of terrorist activity.
    b. Deployment of law enforcement/public safety resources.
    c. Prosecution of crime.
    d. Provision of tactical and/or strategic intelligence to law enforcement. identification and outlining of capabilities of individuals/organizations suspected of having engaged in, or are engaging in, criminal and/or terrorist activities.

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

I. 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.

7. INFORMATION QUALITY ASSURANCE

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

B. [IC]^2 conducts 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 found to be erroneous, misleading, obsolete, or otherwise unreliable.

C. [IC]^2 does not use, gather, or disseminate information it does not have the authority to gather or was obtained using prohibited means.

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

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

8. INFORMATION RETENTION AND DESTRUCTION

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

B. Information received by [IC]^2 analysts and/or the [IC]^2 Supervisor is reviewed to ensure compliance with 28 CFR Part 23; noncompliant information will be purged.

C. All applicable information is reviewed for record retention at least every five (5) years, in compliance with 28 CFR Part 23.
    a. Information found to have no further value or meets the criteria for removal according to 28 CFR Part 23, is destroyed.

D. Basic descriptive information is entered and associated with data or content that is accessed, used, and disclosed:
    a. The name of the originating agency and investigator.
    b. The date the information was collected and the date its accuracy was last verified.

9. INFORMATION SHARING AND DISCLOSURE

A. Access to, or disclosure of, records retained by [IC]^2 is only be provided to persons within [IC]^2 or other governmental agencies who are authorized to access, analyze, and disseminate and holds a legitimate law enforcement, public safety, or criminal justice purpose; information is used for official purposes only.

B. Information gathered and records retained by [IC]^2 is not:

    a. Sold, published, exchanged, or disclosed for commercial purposes.
    b. Disclosed or published without prior notice and/or permission of the contributing agency.
    c. Disseminated to unauthorized persons.

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

D. Information gathered and records retained by [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 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. [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 [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 [IC]^2, in which case [IC]^2 will coordinate with the source agency in responding to the request.

F. Certain law enforcement records, including criminal investigative and criminal intelligence information, may only be disclosed in accordance with Idaho Code §§ 74-124, 74-104(1), and 74-105(1), and any other applicable provisions of the Idaho Public Records Act, Title 74, Chapter 1, Idaho Code.

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

H. [IC]^2 complies with court orders for dissemination of information. Records of all such court orders and information disclosed pursuant to those court orders are maintained.

I. An assessment of information gathered and retained by [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 [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 [IC]^2 and the nature of the information accessed is maintained by [IC]^2.

10. COMPLAINTS AND CORRECTIONS

A. If an individual requests correction of information originating with [IC]^2 that has been disclosed, [IC]^2 Privacy Officer, or designee, informs 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 is 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 $[IC]^2$ (IDAHO CODE § 74-115).

B. $[IC]^2$ informs the individual of the procedure for submitting and resolving such complaints. Complaints are received by the $[IC]^2$ Privacy Officer or $[IC]^2$ Supervisor at 700 S. Stratford Dr., Meridian, Idaho 83642. The $[IC]^2$ Privacy Officer or $[IC]^2$ Supervisor acknowledges the complaint and advises the complainant it will be reviewed; the presence or absence of information is not released, unless otherwise required by law.

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

D. Reasons for refusal to disclose information or denial of requests for corrections are given to the individual who has requested disclosure, or to whom information has been disclosed; procedures for appeal are also outlined (Section 10.A. above).

11. SYSTEMS ACCOUNTABILITY

A. $[IC]^2$ queries made in data applications have a log of the user initiating the query.

B. In conformance with 28 CFR Part 23, all $[IC]^2$ records not updated, are purged every five years.

C. $[IC]^2$ provides an electronic copy of this Policy to all persons who have access to the intelligence system.

D. $[IC]^2$ conducts annual audit and inspection of the information and intelligence contained in its information system(s). The audit is conducted by the $[IC]^2$ Governance Board approved Board of Oversight and Inspection to ensure that: criminal intelligence is handled properly, purged when appropriate, and that access to the fusion center databases and resources are not abused. The audit is conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of $[IC]^2$'s information and intelligence system(s) and ensure compliance by those who have access to, and enter data into, these information systems.

E. $[IC]^2$ personnel or other authorized users 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 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).

State of Idaho General Records Retention Schedule, Series Group #GRS-SEC-005 and #GRS-SEC-008, Activity Reports, Law Enforcement and Crime Analysis Records.

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

Federal Laws:

Brady Handgun Violence Prevention Act, 18 U.S.C. § 925A, 34 U.S.C. §§ 40302, 40901.

Computer Matching and Privacy Act of 1988, 5 U.S.C. § 552a.

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

Crime Identification Technology Act of 1998, 42 U.S.C. § 40301.

Exchange of Criminal History Records for Noncriminal Justice Purposes, 34 U.S.C. §§ 40311 - 40316.

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. §§ 1367-, 2521-, 2701 to 2711-, 3117-, 3121 to 3127.

Fair Credit Reporting Act (FCRA), 15 U.S.C. §§ 1681, 1681a to 1681c, 1861c–1 to 1681c–3, 1681d to 1681s, 1681s–1, 1681s–2, 1681t to 1681x.

Federal Civil action for deprivation of rights, 42 U.S.C. § 1983.

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

HIPAA, Health Insurance Portability and Accountability Act of 1996, 18 U.S.C. §§ 24, 669, 1035, 1347, 1518, 3486; 26 U.S.C. §§ 220, 4980C to 4980E, 6039F, 6050Q, 7702B, 9801 to 9806; 29 U.S.C. §§ 1181 to 1187; 42 U.S.C. §§ 300gg, 300gg–11 to 300gg–13, 300gg–21 to 300gg–23, 300gg–41 to 300gg–47, 300gg–91, 300gg–92, 1320a–7c to 1320a–7e, 1320d, 1320d–1 to 1320d–8, 1395b–5, 1395ddd.

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), 5 U.S.C. § 3598; 6 U.S.C. §§ 123, 194, 321, 413, 458, 485; 8 U.S.C. §§ 1365b, 1776, 1777; 18 U.S.C. §§ 175c, 832, 1038, 2332g, 2332h, 2339D; 22 U.S.C. §§ 2228, 2452c, 2732, 3922a, 4029, 4807, 7536a, 7555; 42 U.S.C. §§ 2000ee, 2000ee–1; 49 U.S.C. § 44925; 50 U.S.C. §§ 1871, 3022 to 3031, 3035, 3036, 3056 to 3058, 3192, 3193, 3321, 3341 to 3343, 3364, 3367, 3506a.

National Child Protection Act of 1993, 34 U.S.C. §§ 40101 – 40104.

National Crime Prevention and Privacy Compact of 1998, 34 U.S.C. §§ 40311 to 40316.

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. §§ 78d–3, 78o-6, 7201, 7202, 7211 to 7220, 7231 to 7234, 7241 to 7246, 7261 to 7266; 18 U.S.C. §§ 1348 to 1350, 1514A, 1519, 1520.

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.