North Dakota State & Local Intelligence Center

Privacy, Civil Rights, and Civil Liberties Policy
January 2011

Table of Contents

	Topic Pages
Mission and Purpose Statement	**2**
Policy Applicability and Legal Compliance	**2**
Governance and Oversight	**2-3**
Common Terms Defined	**3-11**
Personnel Definitions	**12-13**
Information	**13-16**
Acquiring and Receiving Information	**16-17**
Information Quality and Assurance	**17-19**
Data Collation Standards	**19-20**
Sharing and Disclosure	**20-24**
Redress	**24-25**
Security Safeguards	**25-26**
Information Retention and Destruction	**26-27**
Accountability and Enforcement	**27-28**
Training	**29**
Appendix I User Agreement	**30**

Mission and Purpose Statement

Mission Statement - The mission of the North Dakota State & Local Intelligence Center[1] is to collect, store, analyze and disseminate information on crimes, both real and suspected, to the law enforcement community, government officials and private industry concerning dangerous drugs, fraud, organized crime, terrorism and other criminal activity for the purposes of decision making, public safety and proactive law enforcement while ensuring the rights and privacy of citizens.

Purpose Statement - The Purpose of this Privacy Policy is to protect the civil rights and civil liberties of citizens and to ensure that all personnel who have access to ND SLIC information, comply with applicable federal, state, local and tribal laws concerning privacy, civil rights and civil liberties.

Policy Applicability and Legal Compliance

The ND SLIC's Privacy, Civil Rights and Civil Liberties Policy[2] applies to all individuals who and organizations that have access to information retained by the ND SLIC. All ND SLIC personnel, participating agency personnel, private contractors, and other authorized individuals[3] are required to abide by this Privacy Policy and applicable laws which govern the treatment of the information the Center collects, receives, maintains, archives, accesses, or discloses. The ND SLIC intelligence personnel will comply with the Information Sharing Environment Privacy Guidelines, Federal and North Dakota law[4] concerning the appropriate collection, analysis, dissemination and retention of personally identifiable information and intelligence data while complying with and protecting privacy, civil rights, and civil liberties afforded to citizens under the US Constitution and North Dakota State law (the ND SLIC will provide a printed copy of this policy to all Center personnel, participating agencies and individual users). All authorized users are required to provide a signed acknowledgement of receipt of this Privacy Policy and a written agreement to comply with this policy. Nothing in this policy is intended to create a private right of action for any member of the public or alter existing or future federal, state or tribal law requirements.

The ND SLIC has adopted internal operating policies that are in compliance with applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to applicable state and federal privacy, civil rights, and civil liberties laws identified above.

---

[1] Hereinafter referred to as "ND SLIC"
[2] Hereinafter referred to as "Privacy Policy"
[3] Hereinafter referred to as "intelligence personnel"
[4] 28 Code of Federal Regulations (CFR) Part 23; 6 Code of Federal Regulations (CFR) Part 29; North Dakota Century Code Sections 44-04-17.1 through 44-04-31; § 12-60-16.5; § 12-60-16.6; §12.1-35.03; §15.1-24-05; §23-01-05.5; §27-20-51.1; § 32-12.2-11(1); § 39-08-10.1; § 39-08-13(4); §50-25.1-11; § 54-52.1-12; § 57-38-57; § 57-39.2-23; §65-04-15; §27-20-52(1).

Governance and Oversight

The ND SLIC, authorized by Governor John Hoeven on June 27, 2007, in Executive Order 2007-06, is set up to help the efforts of the United States government to establish a national network of Fusion Centers, which will serve as the "central hub" of North Dakota's fusion process and serve as the primary interface between North Dakota and the Federal Government for information collection, analysis and dissemination. The ND SLIC Executive Board, set by Executive Order 2007-06, is comprised of the Adjutant General of the North Dakota National Guard, the Director of the North Dakota Bureau of Criminal Investigation, the Colonel of the North Dakota Highway Patrol and the Director of the North Dakota Division of Homeland Security. The ND SLIC Executive Board has the primary responsibility for the overall operation of the ND SLIC including, but not limited to, its information systems, personnel, and operations.

Daily operations of the ND SLIC are handled by a Coordinator selected by the ND SLIC Executive Board. The Coordinator position is currently held by a Special Agent with the North Dakota Bureau of Criminal Investigation.

The ND SLIC Privacy and Policy Committee is guided by a trained Privacy Officer who is appointed by the ND SLIC Executive Committee. The Privacy Officer receives reports regarding alleged errors and violations of the provisions of this Privacy Policy, receives and coordinates complaint resolution under the Center's redress policy, liaisons with the Information Sharing Environment, ensuring that privacy protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy-enhancing technologies and that the ND SLIC adheres to the provisions of the Information Sharing Environment Privacy Guidelines. The Privacy Officer can be contacted at the following address or phone number: **ndslic@nd.gov or 866-885-8295**.

The ND SLIC is guided by a Privacy and Policy Committee[5] that can liaise with community privacy advocacy groups to ensure that privacy and civil rights are protected within the provisions of this Privacy Policy and within the ND SLIC's information, collection, retention, and dissemination process and procedures, and collaborate with the Privacy Officer on the bi-annual review of the Privacy Policy.

The ND SLIC's Privacy Officer ensures that enforcement procedures and sanctions outlined in "Accountability and Enforcement" are adequate and enforced.

Common Terms Defined

The following terms are used in the course of everyday activity within the ND SLIC and are defined for their use in this Privacy Policy.

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.

1) 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

[5] The ND SLIC Privacy and Policy Committee is comprised of a Legal Representative from the ND Attorney General's Office, the ND SLIC Coordinator, a Legal Representative from the ND National Guard Office and one or more ND SLIC Intelligence Personnel to include the Privacy Officer.

security information, terrorism information, and law enforcement information acquired in the first instance by another ISE participant.

Access Control - The mechanisms for limiting access to certain information based on a user's identity and membership in various predefined groups. Access control can be mandatory, discretionary, or role-based.

Actionable intelligence - Actionable intelligence is a relatively small piece(s) of non-obvious details(s) that can form an initial basis point for hypothesis building.

Acquisition - The means by which an ISE participant obtains information through the exercise of its authorities; for example, through human intelligence collection or from a foreign partner. For the purposes of this definition, acquisition does not refer to the obtaining of information widely available to other ISE participants through, for example news reports or to the obtaining of information shared with them by another ISE participant who originally acquired the information.

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 log-ins and log-outs. 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.

1) Audit trails are a fundamental part of computer security, used to trace (albeit usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

Authorization - The process of granting a person, computer process, or device with access to certain information, services, or functionality. Authorization is derived from the identity of the person, computer process, or device requesting access that is verified through authentication. See Authentication.

Center - Center refers to the ND SLIC and all participating state agencies of the ND SLIC.

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 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.

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 and 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.

Computer Security - Computer Security is the protection of information assets through the use of technology, processes, and training.

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.

Criminal Intelligence Information or Data - 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 acts. The record is maintained in a criminal intelligence system per 28 CFR Part 23.

Critical Infrastructure - Assets, systems, and networks, whether physical or virtual, so vital to the United States and the State of North Dakota that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof.

Critical Infrastructure Information (CII) - Information that is not customarily in the public domain and is related to the security of critical infrastructure or protected systems. CII consists of records and information concerning any of the following:

1) Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or cyber attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety.
2) The ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit.
3) Any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

In accordance with the Critical Infrastructure Information Act of 2002, the implementation of Regulation 6 CFR Part 29 establishes the necessary safeguarding and handling procedures of CII.

Data - Inert symbols, signs, descriptions, characters, or measures.

Data Protection - Data protection encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, use, protection, and disclosure 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.

Electronically Maintained - Information stored by a computer or on any electronic medium from which the information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, or compact disc optical media.

Electronically Transmitted - Information exchanged with a computer using electronic media, such as the movement of information from one location to another by magnetic or optical media, or transmission over the Internet, intranet, extranet, leased lines, dial-up lines, private networks, telephone voice response, or faxback systems. It does not include faxes, telephone calls, video teleconferencing, or messages left on voicemail.

Fair Information Practices - The Fair Information Practices (FIPs) are contained within the Organization for Economic Co-operation and Development's (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. These were developed around commercial transactions and the transborder exchange of information; however, they do provide a straightforward description of underlying privacy and information exchange principles and provide a simple framework for the legal analysis that needs to be done with regard to privacy in

integrated justice systems. Some of the individual principles may not apply in all instances of an integrated justice system.

1) The eight FIPs are:

   A) Collection Limitation Principle
   B) Data Quality Principle
   C) Purpose Specification Principle
   D) Use Limitation Principle
   E) Security Safeguards Principle
   F) Openness Principle
   G) Individual Participation Principle
   H) Accountability Principle

Firewall - A security solution that segregates one portion of a network from another portion, allowing only authorized network traffic to pass through according to traffic-filtering rules.

General Information or Data - Information that may include records, documents, or files pertaining to law enforcement operations, such as computer-aided dispatch (CAD) data, incident data, and management information. It can also be information that is maintained in a records management, CAD system, etc., for statistical/retrieval purposes. Information may be either resolved or unresolved. The record is maintained per statute, rule, or policy.

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.

Identification - A process whereby a real-world entity is recognized and its identity established. Identity is operationalized in the abstract world of information systems as a set of information about an entity that uniquely differentiates it from other similar entities. The set of information may be as small as a single code, specifically designed as an identifier, or a collection of data, such as a given and family name, date of birth, and address. An organization's identification process consists of the acquisition of the relevant identifying information.

Individual Responsibility - Since a privacy notice is not self-implementing, an individual within an organization's structure must also be assigned responsibility for enacting and implementing the notice.

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 can be categorized into four general areas: general data, tips and leads data, suspicious activity reports, and criminal intelligence information.

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.

Intelligence-Led Policing - A process for enhancing law enforcement agency effectiveness toward reducing crimes, protecting community assets, and preparing for responses. ILP provides law enforcement agencies with an organizational framework to gather and use multisource information and intelligence to make timely and targeted strategic, operational, and tactical decisions.

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 ISE-SAR Functional Standard, to have a potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism).

Invasion of Privacy - Invasion of privacy can be defined as intrusion on one's solitude or into one's private affairs, public disclosure of embarrassing private information, publicity that puts one in a false light to the public, or appropriation of one's name or picture for personal or commercial advantage. See also Right to Privacy.

In the Public Domain - Information is said to be "in the public domain" when it is lawfully, properly and regularly disclosed generally or broadly to the public. Information regarding system, facility, or operational security is not "in the public domain." Information submitted with CII that is proprietary or business sensitive, or which might be used to identify a submitting person or entity will not be considered "in the public domain." Information may be "business sensitive" for the purpose whether or not it is commercial in nature, and even if its release could not demonstrably cause substantial harm to the competitive position of the submitting person or entity.

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

Law Enforcement Information - For purposes for the ISE, law enforcement information means any information obtained by or of interest to a law enforcement agency or official that is both:

1) Related to terrorism or the security of the homeland and
2) 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 - Lawful permanent resident is a foreign national who has been granted the privilege of permanently living and working in the United States.

Logs - 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 data. See also Audit Trail.

Maintenance of Information - The maintenance of information applies to all forms of information storage. This includes electronic systems (for example, databases) and non-electronic storage systems (for example, filing cabinets). To meet access requirements, an organization is not required to create new systems to maintain information or to maintain information beyond a time when it no longer serves an organization's purpose.

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 to further an investigation or meet another law enforcement requirement.

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.

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.

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

Personal Data - Personal data refers to any information that relates to an identifiable individual (or data subject). See also Personally Identifiable Information.

Personally Identifiable Information - Personally identifiable information is 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:

1) Personal characteristics (such as 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).
2) A unique set of numbers or characters assigned to a specific individual (including name, address, phone number, social security number, e-mail address, driver's license number, financial account or credit card number and associated PIN number, Automated Integrated Fingerprint Identification System [AIFIS] identifier, or booking or detention system number).
3) Descriptions of event(s) or point(s) in time (for example, information in documents such as police reports, arrest reports, and medical records).
4) Descriptions of location(s) or place(s) (including geographic information systems [GIS] locations, electronic bracelet monitoring information, etc.).

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 - 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 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.

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, dissemination, and access. The purpose of the privacy policy is to articulate that the Center will adhere to those legal requirements and 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.

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

Protected Critical Infrastructure Information (PCII) – refers to all critical infrastructure information, including categorical inclusion PCII, that has undergone the validation process and the PCII Program Office has determined qualifies for protection under the CII Act. All information submitted to the PCII Program Office or Designee with an express statement is presumed to be PCII until the PCII Program Office determines otherwise.

Protected Information - includes personal data about individuals that is subject to information privacy and other legal protections by law, including the U.S. Constitution and the North Dakota constitution; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 23; applicable state and tribal constitutions; and state, local, and tribal laws, ordinances, and codes. Protection may be extended to organizations by ND SLIC policy or state, local, or tribal law.

Public

1) Public includes:
   A) Any person and any for-profit or nonprofit entity, organization, or association;
   B) Any governmental entity for which there is no existing specific law authorizing access to the Center's information;
   C) Media organizations; and
   D) 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.
2) Public does not include:
   A) Employees of the agency;
   B) People or entities, private or governmental, who assist the Center in the operation of the justice information system; and
   C) Public agencies whose authority to access information gathered and retained by the Center is specified in law.

Public Access - 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.

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

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 Center's control.

Repudiation - The ability of a user to deny having performed an action that other parties cannot prove otherwise. For example, a user who deleted a file can successfully deny doing so if no mechanism (such as audit files) can contradict that claim.

Retention - Refer to Storage.

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, or counterterrorism activity.

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 the right to privacy can be the basis for a lawsuit for damages against the person or entity violating a person's privacy.

Role-Based Access - Role-based access is a type of access authorization that uses roles to determine access 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.

Storage

1) 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 types of storage, primary and secondary:
   A) 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 two.
   B) 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.
   C) 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.
2) 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.

Source Agency - Source agency refers to the agency or organizational entity that originates SAR (and when authorized, ISE-SAR) information.

Suspicious Activity - Defined in the ISE-SAR Functional Standard (Version 1.5) as "observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal

activity." Examples of suspicious activity include surveillance, photography of sensitive infrastructure facilities, site breach or physical intrusion, cyberattacks, testing of security, etc.

Suspicious Activity Report (SAR) - Official documentation of observed behavior reasonably indicative of preoperational planning related to 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 IRTPA, all information relating to:

1) 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,
2) 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,
3) Communications of or by such groups or individuals,
4) 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.

1) **Weapons of Mass Destruction (WMD)** – Weapons of Mass Destruction information is 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.
2) **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.

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

Personnel Definitions

1) **Intelligence Personnel**
   A) All ND SLIC staff, analysts and field intelligence personnel (hereinafter referred to as intelligence personnel) are subject to the provisions of this Privacy Policy.
   B) Intelligence personnel include:
      i) **Criminal Intelligence Analysts -** Research and analyze potential terrorism or criminal activity, suspect and incident data;
      ii) **Supervisory Criminal Intelligence Analyst** - First level of supervision over the ND SLIC Criminal Intelligence Analysts and products;
      iii) **Critical Infrastructure Specialists - R**esearch and analyze potential threats to critical infrastructure;
      iv) **State Law Enforcement Representatives -** Research, analyze and bring intelligence to the ND SLIC from their respective parent organizations;
      v) **Local Law Enforcement Representatives -** Research, analyze and bring intelligence to the ND SLIC from their respective parent organizations;
      vi) **Federal Law Enforcement Representatives -** Research, analyze and bring intelligence to the ND SLIC from their respective parent organizations;
      vii) **Law Enforcement Liaison Program Coordinator -** Primary contact with local law enforcement in the effort to gather information for research and analysis in the ND SLIC;
      viii) **Federal Department of Homeland Security Intelligence and Analysis Representative -** Main conduit for classified Federal Department of Homeland Security information coming into the ND SLIC;
      ix) **Coordinator -** Handles ND SLIC day-to-day operations, organization, decision-making and quality control functions.
2) **Department of Emergency Services (DES) Information Technology Department (ITD) Personnel**
   A) Select DES personnel have access to information contained in law enforcement data systems and criminal intelligence data stores for the limited purpose of providing technical assistance.
   B) DES personnel who have access to intelligence data are subject to the provisions of this Privacy Policy.
   C) Notwithstanding any other provisions of this Privacy Policy to the contrary, DES personnel shall not, add, delete, or disseminate criminal intelligence information.

3) **Bureau of Criminal Investigation Information Technology Department (ITD) Personnel**
   A) Select BCI ITD personnel have access to information contained in the law enforcement data systems and criminal intelligence data stores for the limited purpose of providing technical assistance.
   B) BCI ITD personnel who have access to intelligence data are subject to the provisions of this Privacy Policy.
   C) Notwithstanding any other provisions of this policy to the contrary, BCI ITD personnel shall not, add, delete, or disseminate criminal intelligence information.
4) **Authorized Users**
   A) For purposes of this Privacy Policy, authorized persons are Criminal Intelligence Analysts, Supervisory Criminal Intelligence Analyst, Critical Infrastructure Specialists, Law Enforcement Liaison Program Coordinator, Local Law Enforcement Representatives, State Law Enforcement Representatives, Federal Law Enforcement Representatives, Federal Department of Homeland Security Intelligence and Analysis Representative, the ND SLIC Coordinator, field intelligence personnel, public safety officials, certified law enforcement officers, and other criminal justice administrative personnel who:
      i) Are approved for ND SLIC access by the ND SLIC Coordinator and/or Security Officer;
      ii) Are approved for intelligence database access by BCI;
      iii) Meet, at a minimum, the certification requirements for ND SLIC access; and
      iv) Undergo training regarding the system's capabilities as well as the appropriate use and sharing of data accessed through the ND SLIC.
      v) Receive a copy of this Policy and agree in writing to adherence of this Policy, by signing Appendix 1.
5) **Authorized persons**
   A) For purposes of this Privacy Policy, authorized persons are Criminal Intelligence Analysts, Supervisory Criminal Intelligence Analyst, Critical Infrastructure Specialists, Law Enforcement Liaison Program Coordinator, Local Law Enforcement Representatives, State Law Enforcement Representatives, Federal Law Enforcement Representatives, Federal Department of Homeland Security Intelligence and Analysis Representative, the ND SLIC Coordinator, field intelligence personnel, public safety officials, certified law enforcement officers, and other criminal justice administrative personnel in the furtherance of their official duties.
   B) Authorized users may disseminate ND SLIC data to authorized persons as defined in this section only in accordance with the dissemination rules of this Privacy Policy.

Information

1) **The ND SLIC will seek or retain information that:**
   A) Is based upon reasonable suspicion that the information constitutes a credible criminal predicate or a potential threat to public safety; or
   B) Is based upon reasonable suspicion that an identifiable individual or organization has committed, is committing, or is planning to commit criminal conduct or activity that presents a threat to any individual, the community, or the nation; or

C) Is relevant to an active or ongoing investigation and prosecution of suspected criminal incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences by response of any such incident or response; or the prevention of crime reasonably believed likely to occur without such preventative effort; or

D) 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; and

E) Is such that the source of the information is reasonably believed to be reliable and is verifiable and, when appropriate, the limitations on the reliability or veracity of the information is clearly stated; and

F) Is information that was collected in a fair and lawful manner not otherwise prohibited by Law.

2) The ND SLIC will not seek or retain 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, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation. Information related to these factors may be retained if there is a reasonable relationship or relevance to such information and the effort to detect, anticipate, or prevent criminal activity and this information is not the sole basis for retention or indexing. When there is reasonable suspicion that a criminal relationship exists, the information concerning the criminal conduct or activity may be retained or indexed; however, it is the responsibility of the source agency or ND SLIC personnel to ascertain and clearly affirm the relationship to the key element of criminal activity prior to the retention or indexing of the information.

3) The ND SLIC will retain information that is based on reasonable suspicion such as intelligence reports and retain information based on mere suspicion, such as tips, leads and SAR's within a database system only for the length of time allowed under the retention limitations established by 28 CFR Part 23. In addition, ND SLIC may require a contributing agency to justify why any particular tip, lead, intelligence report should remain in the system if it appears to ND SLIC personnel that the information is no longer active or otherwise of intelligence or investigative value. Failure to satisfy ND SLIC's request may result in the information being unilaterally removed from the intelligence database system. Notice of any such removal will be made to the contributor by the Privacy Officer.

4) The ND SLIC applies labels to Center-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 by the Center to include personal information on any individual [See Common Terms Defined definitions of "protected information" and "personal information" in this policy], and, to the extent expressly provided in this policy, includes organizational entities.

B) The information is subject to local, state or federal laws (refer to footnote 4) restricting access, use, or disclosure.

5) The ND SLIC will identify and review protected information that may be accessed from or disseminated by the Center prior to sharing that information through the Information Sharing Environment. Further, the Center will provide notice mechanisms, including but not limited to metadata or data field labels that will enable ISE authorized users to determine the nature of

the protected information and how to handle the information in accordance with applicable legal requirements.

6) The ND SLIC requires certain basic descriptive information to be entered and electronically associated with data (or content) or reports that are to be accessed, used, and disclosed, including terrorism-related information shared through the ISE. The types of information include:

   A) The name of the originating department, or source agency.
   B) The date the information was collected and to the extent possible, the date its accuracy was last verified.
   C) The title and contact information of the person to whom questions regarding the information should be directed and who is accountable for the decision to submit the information and assuring it is believed to otherwise conform to ND SLIC submission standards.
   D) Any particular limitations to the use or disclosure of the information.

7) The ND SLIC will attach (or ensure that the originating agency has attached) specific labels and descriptive metadata to information that will be used, accessed, or disseminated to clearly indicate any legal restrictions on information sharing based on information sensitivity or classification.

8) Outside agency personnel participating with the ND SLIC will, upon receipt of information, review the information to determine its nature and purpose. Once information is reviewed at the ND SLIC, ND SLIC personnel will assign information to categories to indicate the result of the assessment, such as:

   A) Whether the information is general data, tips and leads data, suspicious activity reports, or criminal intelligence information;
   B) The nature of the source (for example, anonymous tip, interview, public records, private sector);
   C) The reliability of the source
      i) Reliable - the source has been determined to be reliable
      ii) Usually Reliable - the information given by the source has typically been reliable
      iii) Unreliable - the reliability of the source is doubtful or has been determined to be unreliable
      iv) Unknown - the reliability of the source cannot be judged or has not as yet been assessed
   D) The validity of the content
      i) Confirmed - the information has been corroborated by a trained law enforcement analyst or officer or other reliable source
      ii) Probable - the information has not been corroborated by a trained law enforcement analyst or officer or other reliable source but is consistent with past accounts and probably true
      iii) Doubtful - the information is of questionable credibility but cannot be discounted based on the knowledge and skills of the reviewer
      iv) Cannot be judged - the information cannot be confirmed at the time of review

E) Unless otherwise indicated by the source or submitting agency, when source reliability is deemed to be “unknown” and content validity “cannot be judged,” users must independently confirm source reliability and content validity with the source or submitting agency or through their own investigation.

F) Due diligence will be exercised by source or submitting agency as well as ND SLIC personnel in determining source reliability and content validity. ND SLIC personnel may reject information as failing to meet any criteria for inclusion, and return such information to the submitting party with an indication of why it was rejected.

G) Information determined to be unfounded will be purged from the intelligence database.

9) At the time a decision is made to contribute information into the intelligence database, ND SLIC personnel or source agency personnel will label it by record, data set, or system of records and be consistent with 28 CFR Part 23 functional standards pursuant to applicable limitations on access and sensitivity of disclosure in order to:

A) Protect an individual’s right of privacy and civil rights and civil liberties;

B) Protect confidential sources and police undercover techniques and methods;

C) Not interfere with or compromise pending criminal investigations; and

D) Provide any legally required protection based on the individual’s status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.

10) At the time information is retained, the date of review of such information to determine whether it should be purged or continued to be retained will be noted (this can be done electronically via date stamping within the intelligence database).

A) Records that are five years old and determined to be no longer active intelligence or criminal investigative information will be purged in accordance with approved records retention schedules, with only statistical information being kept. The time a criminal subject is incarcerated may be used to extend the purge time for the amount of time the defendant was in custody.

11) The retention or classification of existing information will be reevaluated whenever:

A) New information is added that has an impact on access limitations or the sensitivity of disclosure of the information; or

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

C) Information has been developed that suggests the existing information is no longer of intelligence or investigative value or otherwise no longer warrants retention.

12) ND SLIC members are required to adhere to the following practices and procedures for the storage, access, dissemination, retention, and security of tips and leads, and suspicious activity report (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.

A) Store the information using the same storage method used for data that rises to the level of reasonable suspicion and includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information. The storage of ND SLIC intelligence will be through the intelligence database system.

B) Allow access to or disseminate the information using the same (or a more restrictive) access or dissemination method 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).

C) 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 when credible information indicates potential imminent danger to life or property.

D) Retain information 30 days to work a tip or lead to determine its credibility and value, assign a “disposition” label (for example, undetermined or unresolved, cleared or unfounded, meets reasonable suspicion/risen to criminal intelligence) so that an authorized user knows the status and purpose for the retention and will retain the information based upon the retention period associated with the disposition label.

E) Adhere to and follow the Center’s physical, administrative, and technical security measures that are in place for the protection and security of intelligence information. Information will be secured in a system that is the same or similar to the system that secures data that rises to the level of reasonable suspicion.

F) Routinely and regularly review information to determine if it should be purged.

13) Information that has been collected, stored in a database and has a potential terrorism nexus will be shared in accordance with the national standard to include but not limited to the Intelligence Sharing Environment (ISE) Suspicious Activity Report (SAR) Functional Standard (version 1.5).

14) The ND SLIC will keep a record of the originating entity for all information collected by the Center.

Acquiring and Receiving Information

1) Information gathering and research techniques used by the ND SLIC and affiliated members, who have access to the ND SLIC intelligence database, will comply and adhere to the following regulations and guidelines:

   A) The ND SLIC intelligence personnel will comply with Information Sharing Environment Guidelines and will follow 28 CFR Part 23 with regard to criminal intelligence information, adhere to the obligations of law, including Chapter 44-04-18.7 of North Dakota Statutes and comply with the Functional Standard established in the Information Sharing Environment.

2) Regardless of the criminal activity involved, no information which a user has reason to believe may have been obtained in violation of law shall be entered into the intelligence database or submitted to or received by the ND SLIC. If the ND SLIC is notified or otherwise learns that information has been obtained illegally, the information will be removed.

3) Agencies which utilize the ND SLIC and provide information to the Center are governed by state and local laws and rules governing them, as well as by applicable federal laws. The ND SLIC 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 which is not based on misleading information collection practices.

4) The ND SLIC will not directly or indirectly receive, seek, accept, or retain information from:

   A) An individual or nongovernmental information provider who may or may not receive a fee or benefit for providing the information if the Center knows or has reason to believe that the individual or information provider is legally prohibited from obtaining or disclosing the information; or
   B) The source used prohibited or unlawful means to gather the information.

5) When a choice of research techniques is available, information documented should be acquired or researched using the least intrusive feasible means, taking into account such factors as the effect on individuals' privacy and potential damage to reputation.

Information Quality and Assurance

The ND SLIC will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources, is 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 for merging records, refer to section 4 below, has been met. All intelligence information retained by the ND SLIC must be 28 CFR Part 23 compliant.

1) **Data Labeling**

   At the time of retention in the system ND SLIC will apply labels or ensure that the originating agency has applied labels to the information regarding its level of quality (accuracy, completeness, currency, and confidence [verifiability and reliability]).

   A) At the time a decision is made to retain information, it will be labeled to the maximum extent feasible pursuant to applicable limitations on access and sensitivity of disclosure as outlined on page 16, Information Section, subsection 9. The labeling of retained information will be reevaluated when new information is gathered that has an impact on the confidence (validity and reliability) in previously retained information.

2) **Data Ownership**

   A) All data received from or accessed through law enforcement or a public data source is considered to be the property of that source.
   B) All data entered into the BCI intelligence database is considered the property of the ND SLIC and BCI.

3) **Data Accuracy**

A) The ND SLIC will make every reasonable effort to ensure that information will be corrected or deleted from the system, or not used when the 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 Center; 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.

B) Data source agencies retain ownership of their data and each agency is ultimately responsible for the quality and accuracy of its data.

C) If intelligence personnel have cause to believe that data contains an error or deficiency, cannot be verified, or lacks adequate context to the point that the rights of an individual may be affected, they must contact the ND SLIC Privacy Officer who will investigate, in a timely manner, alleged errors and deficiencies (or will notify the originating agency) and correct, delete, or refrain from using protected information found to be erroneous or deficient.

i) The ND SLIC Privacy Officer will notify the originating agency or the originating agency's privacy officer in writing when intelligence personnel review the quality of the information received from an originating agency and identifies data that:

a) May be inaccurate or incomplete;

b) May include incorrectly merged information;

c) May be out of date;

d) Cannot be verified; or

e) Lacks adequate context such that the rights of the individual may be affected.

ii) The ND SLIC Privacy Officer will ensure any erroneous information as noted in c) above is not entered into the Center's intelligence systems.

D) The ND SLIC Privacy Officer will use written or electronic notification to inform recipient agencies when information previously provided to the recipient agency is deleted or changed by the Center because the information is determined to be erroneous, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the rights of the individual may be affected.

4) **Merging Data**

A) Due to the potential harm caused by inaccurate merging of information, data about an individual from two or more sources will not be merged by ND SLIC intelligence personnel unless the identifiers or characteristics, when combined, clearly establish that the information from multiple records is about the same individual. The set of identifiers sufficient to allow merging will consist of all available attributes that can contribute to a higher accuracy of match.

B) If the matching requirements cannot fully be met but there is an identified partial match, the information may be merged only if accompanied by a statement that it has not been adequately established that the information relates to the same individual or organization.

5) **Validation and Verification**

A) Intelligence personnel will respond to any requests from authorized users for validation of previously disseminated data and, when information is identified that may be

inaccurate or incomplete, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context to the point that the rights of an individual may be affected, provide notice to authorized users who are known to have received the information.[6]

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

6) **Data audits and monitoring system use**

A) The ND SLIC Privacy and Policy Committee is responsible for monitoring the use of all ND SLIC data sources to guard against inappropriate or unauthorized use.

B) The ND SLIC Privacy and Policy Committee will investigate misuse of ND SLIC data and conduct or coordinate audits concerning the proper use and security of ND SLIC data.

C) All ND SLIC inquiries by authorized persons will be made available, upon request, to that authorized person's agency.

D) ND BCI will ensure and maintain the integrity of ND SLIC intelligence database in compliance with 28 CFR Part 23.

E) ND BCI has full and complete authoritative review of all information entered into all ND SLIC intelligence databases.

F) Random audits are performed on a continual basis and at least once a year by BCI appointed personnel and ND SLIC Privacy Officer. When information is found to be erroneous or deficient by either the BCI or ND SLIC Privacy Officer, such that an individual's privacy rights are impacted, the BCI appointed personnel and ND SLIC Privacy Officer's responsibilities are limited to notifying the original source agency in writing for their follow-up and correction.[7]

i) The ND SLIC will maintain an audit trail of accessed, requested, or disseminated information.

ii) An audit trail of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request will be kept for a minimum of 5 years.

7) **Information Access and Dissemination**

A) The ND SLIC maintains an access log/audit trail and dissemination record when the database is accessed or information is disseminated from the intelligence systems including terrorism-related information shared through the ISE.

B) Except as otherwise provided in this policy, information and intelligence obtained from or through the ND SLIC will not be:

i) Sold, published, exchanged, or otherwise disclosed, to the public or for commercial purposes;

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

[7] When data is obtained from that source agency, it once again goes through reliability checks prior to labeling. See Section 3 Article VI of this Privacy Policy.

ii) Disseminated to persons not authorized to access or use the information.

iii) Disclosed or published without prior notice to the originating agency that such information is subject to re-disclosure or publication, unless disclosure is agreed to as part of the normal operations of the agency;

a) All re-disclosure or secondary dissemination by the ND SLIC must be logged in accordance with the Sharing and Disclosure Section of this Privacy Policy.

b) External agencies which have received ND SLIC information may not disseminate that information without approval from the originator of the information.

8) **Data Confidentiality**

A) Intelligence personnel shall protect the confidentiality of all data entered or accessed through the ND SLIC.

Data Collation Standards

1) Information acquired or received by the ND SLIC or accessed from other sources will be analyzed only by qualified individuals who have successfully completed a background check and appropriate security clearance, if applicable, and have been selected, approved and trained accordingly.
2) Information subject to collation and analysis is information as defined and identified in the Information Quality and Information Assurance sections of this Policy.
3) Information acquired or received by the ND SLIC or accessed from other sources is analyzed according to priorities and needs and will be analyzed only to:

A) Further crime prevention (including terrorism), enforcement, force deployment, or prosecution objectives and priorities established by the ND SLIC.

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 (including terrorism) activities.

4) The ND SLIC Coordinator has assigned the Privacy Officer and other designees' oversight responsibility to review ND SLIC products prior to dissemination by the center to protect privacy, civil rights, and civil liberties.
5) The ND SLIC 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.

Sharing and Disclosure

1) Credentialed security access will be utilized to control:

A) The information to which a particular group of users can have access based on the group or class.

B) What information a class of users can add, change, delete, or print; and

C) To whom the information can be disclosed and under what circumstances.

2) The ND SLIC intelligence personnel may receive 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 following provisions:

   A) Intelligence personnel must review and vet the information to ensure that it is both legally gathered and, where applicable, determined to have a potential terrorism nexus. Law enforcement officers and intelligence personnel will be trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism.

   B) Intelligence personnel must make reasonable attempts to validate or refute the information to have taken place.

   C) Intelligence personnel must assess the information for sensitivity and confidence by subjecting it to an evaluation 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.

   D) The ND SLIC’s SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved in activities that have been determined to be consistent with criminal activities associated with terrorism will be documented and shared through the ISE. These safeguards are intended to ensure that information that could violate civil rights (race, religion, national origin, ethnicity, etc.) and civil liberties (speech, assembly, religious exercise, etc.) will not be intentionally or inadvertently gathered, documented, processed, and shared.

   E) Intelligence personnel must make sure the information adheres to the current version of the ISE-SAR Functional Standard for its SAR process, including the use of a common standard reporting format and accepted data collection codes and a sharing process that complies with the ISE-SAR Functional Standard for suspicious activity potentially related to terrorism.

3) Access or disclosure of records retained by the ND SLIC will be provided only to persons within the ND SLIC or in other governmental agencies who are authorized to have access and only for legitimate law enforcement purpose, public protection, public prosecution, or public health (only for public protection), or justice purposes and only for the performance of official duties in accordance with law and procedures applicable to the agency for which the person is working. An audit trail sufficient to allow the identification of each individual who accessed information retained by the Center and the nature of the information accessed will be kept by the Center.

4) Records retained by the ND SLIC 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 Center and the nature of the information accessed will be kept by the Center.

5) Information gathered and records retained by the ND SLIC may be accessed or disclosed 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 five years for this type of request which will include the requestor information, the specific purpose for the request and what information was requested.

6) **Audit Logs:**

C) **Intelligence Database audit logs**

i) Queries to intelligence database will be logged by the system and identify the user initiating the query. The dissemination log must contain;

ii) A description of the information queried (including the identity or identities to whom the information relates);

iii) The date the information was queried;

iv) The individual who conducted the query;

v) The authorized person to whom the information was disseminated.

7) Information gathered or collected and records retained by the ND SLIC 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 center's mission and is not exempt from disclosure by law. Such information may be disclosed only in accordance with the law and procedures applicable to the center for this type of information. An audit trail sufficient to allow the identification of each individual member of the public who accessed or received information retained by the center and the nature of the information accessed will be kept by the center.

8) ISE-SAR information posted to the shared space by the ND SLIC may be disclosed to a member of the public only if the information is defined by law to be public record or otherwise appropriate for release to further the ND SLIC mission and is not exempt from disclosure by law.

9) ND SLIC may possess information that is exempt from public disclosure or confidential and not subject to inspection or disclosure except as authorized under federal statutes, applicable federal regulations, and state statutes.

A) **Confidential and Exempt Information**

The following state and federal laws are laws of general applicability for non-disclosure of records and information:

N.D.C.C. ch. 6-08.1(Financial Institution Customer Information); § 6-09-35 (Bank of North Dakota Records); § 10-04-16.1 (Securities Investigations); § 11-19.1-11 (Autopsy Reports); § 12-44.1-28 (Correctional Facility Inmate Records); § 12-47-36 (Department of Corrections and Rehabilitation Offender Records); § 12-55.1-11 (Pardon Advisory board Records); § 12-59-04 (Parole Board Records); § 12.1-34-02(4) & (17) (Confidential Victim Information); § 14-07.1-18 (Domestic Violence or Sexual Assault Records); §14-07.3-02 (Minor's private counseling information); § 15.1-19-14 (School Law Enforcement Unit Records); § 15.1-24-04 (student medical, treatment, and individual records); § 19-03.1-35 (pharmacy research or patient identity records); § 23-01-05.5 (Autopsy Reports); § 23-01.1-05 (Health Care Data Committee Records); ch. 23-01.3 (Protected Health Information); § 23-02.1-27 (Birth, Death, and Fetal Death Records); §§ 23-07-02.1 and § 23-07-02.2 (Reports of Human Immunodeficiency Virus Infection) ; § 23-07-20.1 (Disease Control Records); §23-07-21 (Penalties for violations of disease control requirements and for disclosure of confidential information); § 23-07.5-02 (Records of court hearings for testing for blood borne pathogens); § 23-07.5-06

(Prohibition of disclosure of test result of blood borne pathogens); §§ 23-07.5-07 and 23-07.5-08 (Civil and criminal penalties for disclosure of test results of blood borne pathogens); § 23-07.6-11 (Communicable Disease Confinement Records); § 25-03.1-43 (Records of persons civilly committed for mental illness or chemical dependency); ch. 25-03.3 (Records for civilly committed sexually dangerous individuals); § 27-20-51 (Juvenile Court Records); § 27-21-12 (Division of Juvenile Services Records); § 32-12.2-11 (State Risk Management Fund Records); § 32-12.2-12 (State Agency Loss Control Committee Records and Meetings); § 32-12.2-14 (State Risk Management Motor Vehicle Accident Review Board Records and Meetings); § 37-18-11 (Department of Veterans Affairs Records); § 39-08-13(4)(Officer's opinion on traffic accident form); § 39-08-14 (Accident reports by persons involved in accidents or by garages and proof of financial responsibility); § 39-16-03.1 (Driver's record or abstract); ch. 39-33 (Driver's License Restricted Personal Information); § 44-04-18.1 (Public employee personal, medical, and employee assistance records); § 44-04-18.4 (Trade secret, proprietary, commercial, and financial information): § 44-04-18.5 (Computer Software Programs); § 44-04-18.6 (Legislative Records and Information); § 44-04-18.8 (Examination questions and procedures); § 44-04-18.9 (Financial Account Numbers); § 44-04-18.12 (Cooperative investigations and litigation); § 44-04-18.13 (Lists of minors); § 44-04-18.14 (Follow-up information on North Dakota Education and Training System); § 44-04-18.15 (Higher Education Fundraising and Donor Records); § 44-04-18.16 (Patient Records and Student Health Services and University System Clinics); § 44-04-18.17 (Personal Information in Consumer Complaint); § 44-04-18.18 (Autopsy Images); § 44-04-18.19 (Records of Recipients of Economic Assistance or Support); § 44-04-18.21 (Electronic e-mail addresses and telephone numbers); § 44-04-19.1 (Attorney Work Product); § 44-04-28 (Social Security Numbers); § 44-04-29 (University of North Dakota School of Law Clinical Education Program Client Files); § 44-04-30 (Records of Fire Departments and Rural Fire Protection Districts); § 50-25.1-11(Child Abuse and Neglect Records);§ 54-12-24 (Crime Laboratory Toxicology Records); § 54-23.4-17 (Crime Victims Compensation Records); §§ 54-52.1-11 and 54-52.1-12 (Group insurance and medical records); 17 U.S.C. § 107(Copyright and Fair Use); 20 U.S.C. § 1232g (Family Educational Right to Privacy Act); 42 C.F.R. part 2 (Drug and alcohol treatment records); 45 C.F.R. parts 160 and 164 (health care and treatment records).

B) **Law Enforcement, Investigatory and Criminal Intelligence Information, and Criminal History Record Information**

Law enforcement, investigatory and criminal intelligence information, and criminal history record information is not subject to inspection or disclosure except as authorized under federal statutes, applicable federal regulations, and state statutes, including: N.D.C.C. §§ 12-60-16.5 and 12-60-16.6 (Criminal History Record Information); § 12.1-32-15(13) and (15) (Sex offender and felony offender against children conviction and registration information); § 12-60-24 (Criminal History Record Checks-FBI Criminal History Record Information); § 12.1-35-03 (Child Victim and Witness Information); § 15.1-24-05 (Law Enforcement Reporting Obligations to School Chemical Abuse Preassessment Team ; § 16.1-19-06 (Investigations of Public Officer's Statement of Interest); ch. 19-03.5 (Prescription Drug Monitoring Program Records); § 27-20-31.1 (Record of Suspension of Juvenile Driving Privileges) § 27-20-51.1 (Disclosure of Information to Apprehend Juvenile); § 27-20-52 (Law Enforcement and Correctional Facility Records of Juveniles); § 27-20-53 (Children's Fingerprints and Photographs); § 27-20-54 (Destruction of Juvenile Records); § 29-05-32 (Confidential arrest warrant and complaint information); § 31-13-06 (DNA law enforcement data base records); § 37-

17.1-06(6)(f) (State Homeland Security Sensitive and Proprietary Logistical Data); § 44-04-18.3(1)-(4)(records of juvenile court supervisors, department of corrections employees, undercover law enforcement, confidential informants, and law enforcement schedules); § 44-04-18.7 (Criminal Intelligence and Investigative Information); § 44-04-18.20 (Domestic Violence Records).

C) **Security System Plans, Public Health and Security Plans, and Computer Passwords and Security Information.**

i) Security system plans are exempt from public disclosure. See N.D.C.C. § 44-04-24. Security system plans include:

a) All records, information, photographs, audio and visual presentations, schematic diagrams, surveys, recommendations, communications, or consultations or portions of any such plan relating directly to the physical or electronic security of a public facility, or any critical infrastructure, whether owned by or leased to the state or any of its political subdivisions, or any privately owned or leased critical infrastructure if the plan or a portion of the plan is in the possession of a public entity.

b) Threat assessments; vulnerability and capability assessments conducted by a public entity, or any private entity.

c) Threat response plans; and emergency evacuation plans.

ii) N.D.C.C. § 44-04-25: Public health and security plans are exempt from public disclosure. Public health and security plans include those plans and only those portions of the records, information surveys, communications, and consultations used o produce the plans relating to the protection of the public or public officials against threats of violence or other harm.

iii) N.D.C.C. § 44-04-26: Those portions of a meeting which would reveal a security system plan, a public health or security plan, or a portion of any such plan that are exempt under N.D.C.C. §§ 44-04-24 or 44-04-25 are exempt from the open meeting requirements of N.D.C.C. § 44-04-19.

iv) N.D.C.C. § 44-04-27: Computer passwords and security information of a public entity are confidential. Information that is confidential under this section includes security codes, passwords, combinations, or security-related plans used to protect electronic information or to prevent access to computers, computer systems, or computer or telecommunications networks of a public entity.

10) The ND SLIC shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information unless otherwise required by law.

Redress

1) Information that is retained by the ND SLIC, to include intelligence database records and ISE-SAR information, is considered active intelligence or criminal investigative information and, therefore, is exempt from public disclosure. If an individual wants to review information that has been documented in an intelligence file or system or as part of an investigative case management system, a formal public records request must be made through the North Dakota Attorney General's Office, Bureau of Criminal Investigation. Information on "Open Records" laws can be found at http://www.ag.state.nd.us/OpenRecords/ORM.htm. Upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity and subject to the conditions specified in paragraph two (2), below, 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 ND SLIC. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information. The Center'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.

2) The existence, content, and source of the information will not be made available to an individual, when there is legal basis for denial. To the extent allowed by law, information will not be verified or released if:

   A) The disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution[8];
   B) The disclosure would endanger the health or safety of an individual, organization, or community[9];
   C) The information is in a criminal intelligence system[10].

3) If a public records request was made through the North Dakota Attorney General's Office, Bureau of Criminal Investigation, and the decision was made to release information, any complaints or objections to the accuracy or completeness of information retained about him

---

[8] N.D.C.C. §12-60-16.5; §12-60-16.6; § 12.1-32-15(13) and (15); § 12.1-35-03; § 15.1-24-05; § 27-20-51.1, § 27-20-52; § 44-04-18.3(1)-(4); § 44-04-18.7(1) through (7) 6-08.1; § 12-44.1-28; § 12-47-36; § 15.1-19-14; ch. 23-01.3; § 23-07-02.1; § 23-07-02.2; § 23-07-20.1; § 23-07.5-06; § 23-07.5-08; § 23-07.6-11; § 25-03.1-43; § 25-03.3-03(2); § 25-03.3-05; § 27-21-12; § 32-12.2-11; § 32-12.2-14 § 39-01-10.1(2); § 39-06-14(1); § 39-08-13(4); ch. 39-33; § 44-04-18.1; §§ 44-04-18.4 through 44-04-18.6; § 44-04-18.8; § 44-04-18.9; §§ 44-04-18.12 through 44-04-18.14; §§ 44-04-18.17 through 44-04-18.21; §§ 44-04-28 through 44-04-30; § 50-25.1-11; § 54-52.1-12; 17 U.S.C. § 107; 20 U.S.C. § 1232g; 42 C.F.R. part 2; 45 C.F.R. parts 160 and 164.

[9] N.D.C.C. § 44-04-24. 44-04-25, 44-04-24, 44-04-25, 44-04-19 and 44-04-27.

[10] N.D.C.C. §12-60-16.5; §12-60-16.6; § 12.1-32-15(13) and (15); § 12.1-35-03; § 15.1-24-05; § 27-20-51.1, § 27-20-52; § 44-04-18.3(1)-(4); § 44-04-18.7(1) through (7) 6-08.1; § 12-44.1-28; § 12-47-36; § 15.1-19-14; ch. 23-01.3; § 23-07-02.1; § 23-07-02.2; § 23-07-20.1; § 23-07.5-06; § 23-07.5-08; § 23-07.6-11; § 25-03.1-43; § 25-03.3-03(2); § 25-03.3-05; § 27-21-12; § 32-12.2-11; § 32-12.2-14 § 39-01-10.1(2); § 39-06-14(1); § 39-08-13(4); ch. 39-33; § 44-04-18.1; §§ 44-04-18.4 through 44-04-18.6; § 44-04-18.8; § 44-04-18.9; §§ 44-04-18.12 through 44-04-18.14; §§ 44-04-18.17 through 44-04-18.21; §§ 44-04-28 through 44-04-30; § 50-25.1-11; § 54-52.1-12; 17 U.S.C. § 107; 20 U.S.C. § 1232g; 42 C.F.R. part 2; 45 C.F.R. parts 160 and 164.

or her should be made in writing and handled by the North Dakota Bureau of Criminal Investigation. The individual would be required to provide a written request to modify the documentation, remove the record and provide adequate reasoning for the request. The information would then be submitted to the ND SLIC for compliance with the decision. A record will be kept of all decisions made for corrections and the resulting action, if any.

A) If an individual has complaints or objections to the accuracy or completeness of information about him or her that originates in another agency, the ND SLIC will contact the originating agency to inform them of the complaint when appropriate under applicable law, or refer the requestor to the originating agency. The ND SLIC will keep a record of the complaints and track the resulting action taken by the originating agency.

B) If an individual has complaints or objections to the accuracy or completeness of terrorism-related protected information that:

   i) Is exempt from disclosure
   ii) Has been or may be shared in the ISE.
   iii) Is held by ND SLIC and allegedly has resulted in demonstrable harm to the complainant,

C) The ND SLIC will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the ND SLIC's Privacy Officer at the following: ndslic@nd.gov or 866-885-8295. The Privacy Officer 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 Center, the Privacy Officer 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 Center that is the subject of a complaint will be reviewed within 30 days and confirmed or corrected/purged if determined to be inaccurate or incomplete, to include incorrectly merged information, or to be out of date. If there is no resolution within 30 days, the Center will not share the information until such time as the complaint has been resolved. A record will be kept by the Center of all complaints and the resulting action taken in response to the complaint.

4) The individual to whom information has been disclosed will be provided with a justification and the procedures for appeal; if the request for correction is denied by the ND SLIC or the originating agency, the individual will be informed of the procedures for correcting or modifying the information. All appeals with be handled by the North Dakota Attorney General's Office. A record will be kept of all requests and of what information is disclosed to an individual.

5) If an individual has complaints or objections to the accuracy or completeness of ISE-SAR information resulting in specific, demonstrable harm to said individual, and that such information about him or her is alleged to be held by the ND SLIC, the ND SLIC**,** must 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.

6) The ND SLIC will acknowledge the complaint and state that it will be reviewed, but will not confirm the existence of any ISE-SAR that contains information in privacy fields that identifies the individual. However, any personal information will be reviewed and corrected in or deleted from the ISE-SAR shared space if the information is determined to be erroneous, includes incorrectly merged information, or is out of date.

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

Security Safeguards

1) ND Bureau of Criminal Investigation and ND Department of Emergency Services, whose department heads sit on the ND SLIC Executive Board, have Information Security Officers who support the ND SLIC and are trained to handle network access/security and manage firewalls that are in place to prevent unauthorized agencies or entities from accessing ND SLIC resources.

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

3) Physical Safeguards - The ND SLIC systems shall be located in a physically secured area that is restricted to designated authorized personnel.

   A) Only designated authorized personnel will have access to information stored in the ND SLIC data systems.
   B) All authorized visitors will be escorted by designated authorized personnel for the duration of their visit.
   C) Disaster Recovery - ND Bureau of Criminal Investigation and ND Department of Emergency Services have appropriate disaster recovery procedures for ND SLIC data outlined at their respective agencies.

4) The ND SLIC will adhere to and follow the ND SLIC physical, administrative, and technical security measures that are in place for the protection and security of tips, leads and SAR information. Tips, leads and ISE-SAR information will be kept in a secure system such as e-Guardian or a similar system that secures data that rises to the level of reasonable suspicion.

5) The ND SLIC Executive Board has appointed the ND Critical Infrastructure Program Manager as the ND SLIC Physical Security Officer.

6) Security breaches and security breach notification – BCI and DES will monitor and respond to security breaches or breach attempts.

   A) In the event that ND SLIC personnel become aware of a breach of the security of unencrypted personal information, The ND SLIC Privacy Officer will notify BCI or DES and the individual about whom personal information was or is reasonably believed to have been obtained by an unauthorized person and access to which threatens the physical or financial harm to the person.

B) Any necessary notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or any measures necessary to determine the scope of the release of information and if necessary, to reasonably restore the integrity of any information system affected by this release.

7) Access to ND SLIC information will be granted only to Center 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.

8) An access audit log/trail or dissemination record is required when the database is accessed or information is disseminated from the intelligence system including terrorism-related information shared through the ISE-SAR. The database log/audit trail automatically captures the ND SLIC user. The ND SLIC user must manually enter the requesting/submitting agency and officer's name. Audit log/trail or dissemination records are stored in the ND SLIC intelligence database.

9) Risk and vulnerability assessments are stored separately from law enforcement, intelligence, and public data. Risk and vulnerability assessments are not available to the public.

Information Retention and Destruction

1) All applicable information will be reviewed for record retention (validation or purge) by ND SLIC at least every five (5) years, as provided by 28 CFR Part 23.

2) When information has no further value or meets the criteria for removal according to the ND SLIC retention and destruction policy, it will be purged, destroyed, and deleted or returned to the submitting (originating) agency.

   A) ND SLIC intelligence databases will automatically run checks for data that has met the five-year retention period. Data that has not been validated is purged.
   B) If the information has not been updated and/or validated, it must be removed from the system at the end of the retention period. Material purged from the intelligence system shall be destroyed.[11]
   C) Non-intelligence information will be maintained and/or destroyed in accordance with the North Dakota Open Records Laws.

3) Destruction requirements for Protected Critical Infrastructure Information (PCII): Original PCII materials may not be destroyed without the approval of the DHS PCII Program Manager. The North Dakota Department of Emergency Services will likely only have copies of PCII and not original PCII materials.

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

A) Copies of validated PCII shall be destroyed when they are no longer needed. No approval is required to destroy copies of PCII materials. Destruction of such documents may be recorded on the PCII Tracking Log. PCII working papers will be destroyed when the final conclusions have been created from them and validated as PCII. No approval is required to destroy these PCII working papers, and their destruction does not need to be recorded.

   i) No approval will be required from the originating agency before information held by the ND SLIC is destroyed or returned in accordance with this policy or as otherwise agreed upon with the originating agency.

4) When information has no further value or meets the criteria for removal, no approval will be required from the originating agency before information held by the ND SLIC is destroyed or returned in accordance with this policy or as otherwise agreed upon with the originating agency.

5) Destruction Methods: Careful consideration must be given to destruction of PCII material/information to prevent inadvertent disclosure of sensitive information. PCII material must be destroyed by authorized means and approved methods (see table below) to preclude recognition and reconstruction of the information.

Approved Destruction Methods for PCII

Type of Media	Approved Destruction Methods
Paper	Shred or Burn
Electronic File	Delete and empty recycle bin
Magnetic Media	Degauss or shred
Compact Discs	Shred and grind
Thumb Drives/Memory Sticks	Wipe and erase data
Microfiche: Audio/Video Tapes	Chemical (e.g., acetone bath) or shred

6) Notification of proposed destruction or return of records may or may not be provided to the originating agency by the ND SLIC, depending on the relevance of the information and any agreement with the originating agency.
7) The ND SLIC will retain a record of dates when information is to be removed (purged) if not validated prior to the end of its five-year period, notice will be given to the submitter at least 30 days prior to the required review and validation/purge date.

Accountability and Enforcement

1) Information System Transparency

   A) The approved Privacy Policy will be displayed for general view on the ND SLIC website at http://www.nd.gov/des/uploads/resources/659/privacypolicy-ndslic.pdf. Intelligence personnel and agencies with access to ND SLIC data must follow all applicable state and federal laws and regulations. Inquiries and complaints about privacy, civil rights, and civil liberties protections will be directed to the ND SLIC Privacy Officer. The Privacy Officer can be contacted at: ndslic@nd.gov or 866-885-8295.

2) Accountability
   A) All intelligence personnel are required to abide by this Privacy Policy and applicable laws which govern the treatment of the information the ND SLIC collects, receives, maintains, archives, accesses, or discloses.
   B) User Compliance
      i) The ND SLIC Privacy Policy Committee is responsible for monitoring the use of all ND SLIC data sources to guard against inappropriate or unauthorized use.
      ii) The ND SLIC Privacy Policy Committee will investigate misuse of ND SLIC data and conduct or coordinate audits with the BCI concerning the proper use and security of ND SLIC data.
         (1) All entries of new ND SLIC intelligence database users are reviewed by the ND SLIC Privacy and Policy Committee for the first 60 days.
         (2) The ND SLIC Privacy and Policy Committee will randomly review 1% percent of all ND SLIC intelligence database entries annually.
   C) Violations
      i) When the ND SLIC Privacy and Policy Committee learns of a violation of policy, laws, or regulations concerning the use of ND SLIC data, it must notify the chief executive of the offending agency in writing. Agencies must take action to correct such violations and provide an assurance in writing to the ND SLIC Coordinator or Privacy Officer that corrective action has been taken.
      ii) Any suspected or documented misuse of ND SLIC information discovered by or reported to a law enforcement agency must be reported by that agency to the ND SLIC Privacy Officer.
   D) The ND SLIC Privacy Policy will be reviewed by the ND SLIC Coordinator and Privacy Officer bi-annually to identify areas that need to be amended or changed.

3) Enforcement
   A) If an authorized user is found to be in noncompliance with the provisions of this Privacy Policy regarding the collection, use, retention, destruction, sharing, classification, or disclosure of information, the ND SLIC Coordinator will:
      i) Suspend or discontinue access of the user to the information;
      ii) Refer the user to their parent agency for disciplinary procedures;
      iii) Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of this policy.

4) The ND SLIC reserves the right to restrict the qualifications and number of personnel having access to Center information and to suspend or withhold service and deny access to any participating agency or participating agency personnel violating the Center's privacy policy.

Training

1) The ND SLIC has adopted the Bureau of Justice Assistance 28 CFR Part 23 online training as the education and training standard for its intelligence personnel.
   A) Training is provided on this Privacy Policy to all intelligence personnel.

B) The ND SLIC will provide training to personnel authorized to access and/or disseminate data, including terrorism-related data.

C) The ND SLIC will provide special training regarding the Center's requirements, policies for collection, use, and disclosure of protected information to personnel authorized to share protected information through the Information Sharing Environment.

D) This Privacy Policy has been viewed and approved by a licensed attorney from the North Dakota Attorney General's Office.

E) Private sector personnel in contractual relationships with the ND SLIC will receive training on this Privacy Policy.

2) The ND SLIC's privacy policy training program will cover:

A) Purposes of the privacy, civil rights, and civil liberties protection policy.

B) Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the Center.

C) Originating and participating agency responsibilities and obligations under applicable law and policy.

D) How to implement the policy in the day-to-day work of the user.

E) The impact of improper activities associated with infractions within or through the agency.

F) Mechanisms for reporting violations of Center privacy protection policies and procedures.

G) The nature and possible penalties for policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.

.

Appendix I

I, the undersigned, certify that I have read the "ND SLIC Privacy Policy" and will comply with it; and that I am familiar with my responsibilities as an authorized user of any databases I use. I will retain a copy of this document for future reference. I also certify that I will follow the specific procedures for using and protecting the information held within ND SLIC databases and protecting individuals civil rights and civil liberties.

User Name: _____

User Signature: _____

Date: _____

Privacy Policy Officer Signature: _____

Date: _____