North Dakota State & Local Intelligence Center

Privacy, Civil Rights, and Civil Liberties Policy (P/CRCL)
2019

Table of Contents

Mission and Purpose Statement

Mission Statement - The mission of the North Dakota State & Local Intelligence Center[1] is to gather, evaluate, analyze and disseminate information and intelligence data (records) on crimes, both real and suspected, to the law enforcement community, government officials and private industry concerning dangerous drugs, fraud, organized crime, terrorism, cyber and other criminal activity for the purposes of decision making, public safety and proactive law enforcement while ensuring the rights and privacy of citizens[2].

Purpose Statement - The purpose of this privacy, civil rights, and civil liberties (P/CRCL) protection policy is to promote the NDSLIC and user conduct that complies with applicable federal, state, local, tribal, and territorial law (refer to the Common Terms Defined sections) and assists the center and its users in:

- Increasing public safety and improving national security
- Minimizing the threat and risk of injury to specific individuals
- Minimizing the threat and risk of physical or financial injury to law enforcement and others responsible for public protection, safety, or health
- Minimizing the threat and risk of damage to real or personal property
- Protecting individual privacy, civil rights, civil liberties, and other protected interests
- Protecting the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information
- Minimizing the reluctance of individuals or groups to use or cooperate with the justice system
- Supporting the role of the justice system in society
- Promoting governmental legitimacy and accountability
- Not unduly burdening the ongoing business of the justice system
- Making the most effective use of public resources allocated to public safety Agencies

Policy Applicability and Legal Compliance

The NDSLIC's Privacy, Civil Rights and Civil Liberties Policy(P/CRCL)[3] applies to all individuals who and organizations that have access to information retained by the NDSLIC. All NDSLIC personnel, participating agency personnel, private contractors, and other authorized individuals[4] are required to abide by this P/CRCL Policy and applicable laws which govern the treatment of the information the Center gathers, receives, maintains, archives, accesses, or discloses. The NDSLIC intelligence personnel will comply with the Information Sharing Environment (ISE) Privacy Guidelines[5], Federal and North Dakota law[6] concerning the appropriate gathering,

[1] Hereinafter referred to as "NDSLIC"
[2] This includes implementing appropriate privacy and civil liberties safeguards as outlined in the principles of the Privacy Act of 1974, as amended, to ensure that the information privacy and other legal rights of individuals and organizations are protected (refer to definitions of "Fair Information Practice Principles" [FIPPs] and "Protected Information" in the Common Terms defined section).
[3] Hereinafter referred to as "P/CRCL Policy"
[4] Hereinafter referred to as "intelligence personnel"
[5] Hereinafter referred to as "ISE"
[6] 28 Code of Federal Regulations (CFR) Part 23; 28 Code of Federal Regulations (CFR) Part 20; 6 Code of Federal Regulations (CFR) Part 29; North Dakota Century Code Sections 44-04-17.1 through 44-04-31; §12-47-36; § 12-60-16.5; § 12-60-16.6; §12.1-35-03; §15.1-24-05; §23-01-05.5; §27-20-51.1; §27-21-12; § 32-12.2-11(1); § 39-08-10.1; § 39-08-13(4); ch. 39-33; §50-25.1-11; § 54-52.1-12; § 57-38-57; § 57-39.2-23; §65-04-15; §27-20-52(1).

analysis, dissemination and retention of personally identifiable information and intelligence data while complying with and protecting privacy, civil rights, and civil liberties afforded to individuals in the United States under the US Constitution and North Dakota State law (the NDSLIC 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 P/CRCL 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 NDSLIC has adopted internal operating policies that are compliant 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.

Governance and Oversight

The NDSLIC, re-authorized by Governor Jack Dalrymple on March 25, 2014, in Executive Order 2014-06, 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 gathering, analysis, and dissemination. The NDSLIC 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, Director of the North Dakota Division of Homeland Security, and the North Dakota Information Technology Department Chief Information Officer. The NDSLIC Executive Board has the primary responsibility for the overall operation of the NDSLIC including, but not limited to, its information systems, personnel, and operations.

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

The NDSLIC Privacy and Policy Committee is guided by a trained Privacy Officer who is appointed by the NDSLIC Executive Committee. The Privacy Officer Position is held by the Chief of Administration within the NDSLIC. The committee will annually review and update the P/CRCL policy in response to changes in law and implementation experience, including the results of audits and inspections, and may solicit input from stakeholders on the development of or proposed updates to the policy. The Privacy Officer can be contacted at the following address or phone number: **ndslic@nd.gov or** 701-328-8172.

The NDSLIC is guided by a Privacy and Policy Committee[7] that oversees and advises the NDSLIC's Information Liaison Officer (ILO) program. The ILO can liaise with community privacy advocacy groups to ensure that privacy and civil rights are protected within the provisions of this P/CRCL Policy and within the NDSLIC's information gathering, retention, and dissemination process and procedures, and collaborate with the Privacy Officer on the annual review of the P/CRCL Policy. The committee will annually review and update the P/CRCL policy in response to

[7] The NDSLIC Privacy and Policy Committee is comprised of a Legal Representative from the ND Attorney General's Office, the NDSLIC Director, a Legal Representative from the ND National Guard Office, one or more NDSLIC Intelligence Personnel, and the NDSLIC's Privacy Officer.

changes in law and implementation experience, including the results of audits and inspections, and will solicit input from stakeholders on the development of or proposed updates to the policy.

The NDSLIC'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 NDSLIC and are defined for their use in this P/CRCL Policy.

Access - Information access is being able to get to (usually having permission to use) particular information on a computer. Web access means having a connection to the Internet through an access provider or an online service provider.

1) With regard to the ISE, access refers to the business rules, means, and processes by and through which ISE participants obtain terrorism- associated information, to include homeland 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 gathering 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.

Agency - See Originating Agency, Owning Agency, Participating Agency, Source Agency, Submitting Agency.

Analysis (law enforcement) - The review of information and its comparison to other information to determine the meaning of the data in reference to a criminal investigation or assessment.

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.

Biometrics - A general term used alternatively to describe a characteristic or a process. (1) As a characteristic: a measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition. (2) As a process: automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics. See

Fusion Center Privacy, Civil Rights, and Civil Liberties Policy Development, Version 3.0

36

Glossary, Facial Identification Scientific Working Group (FISWG), Version 1.1, February 2, 2012, https://www.fiswg.org/FISWG_Glossary_v1.1_2012_02_02.pdf.

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

Civil Liberties - According to the U.S. Department of Justice's Global Justice Information Sharing Initiative, the term "civil liberties" refers to fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights—the first ten amendments to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference.

Collect - For purposes of this document, "gather" and "collect" mean the same thing.

Civil Rights - The term "civil rights" refers to those rights and privileges of equal protection that government entities must afford to all individuals in the United States regardless of race, ethnicity, gender, national origin, religion, sexual orientation, gender identity, or other characteristics unrelated to the worth of the individual. Protection of civil rights means that government entities will act to ensure that individuals are not discriminated against on the basis of any federally or state protected characteristic. For example, a state may have constitutional or statutory language regarding parental status. Generally, the term "civil rights" involves positive (or affirmative) government action to protect against infringement, 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 - Refers to the obligations of individuals and institutions to appropriately use information and data under their control once they have been disclosed to them and in accordance with applicable data security laws and policies.

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

Criminal Activity - A behavior, an action, or an omission that is punishable by criminal law.

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 & 28 CFR Part 20.

Critical Infrastructure (CI) - 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. [8]

[8] Source: https://www.dhs.gov/sites/default/files/publications/pcii_final_rule_federal_register9-1-06-2_508.pdf

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

Data Breach - The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for a purpose other than the authorized purpose.

- The center's response to a data breach may be addressed in state law or agency policy. This may include incidents such as:
- Theft or loss of digital media—including computer tapes, hard drives, or laptop computers containing such media—upon which such information is stored unencrypted; posting such information on the Internet.
- Unauthorized employee access to certain information.
- Moving such information to computer otherwise accessible from the Internet without proper information security precautions.
- Intentional or unintentional transfer of such information to a system that is not completely open but is not appropriately or formally accredited for security at the approved level, such as unencrypted e-mail.
- Transfer of such information to the information systems of a possibly hostile agency or an environment where it may be exposed to more intensive decryption techniques.

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

Disclosure - The release, transfer, provision of access to, sharing, publication, or divulging of PII in any manner—electronic, verbal, or in writing—to an individual, agency, or an 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 purpose(s) 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, compact disc optical media, or cloud technologies. 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.

Evaluation - An assessment of the reliability of the source and accuracy of the raw data.

Fair Information Practice Principles (FIPPs)—FIPPs are a set of internationally recognized principles that inform information privacy policies both within government and the private sector. Although specific articulations of the FIPPs vary and have evolved since their genesis in the 1970s, core elements are consistent among nations, states, and economic sectors. These core elements are incorporated into information privacy laws, policies, and governance documents around the world. They provide a straightforward description of underlying privacy and information exchange principles and a simple framework for the legal use that needs to be done with regard to privacy in integrated justice systems. Because of operational necessity, it may not always be possible to apply all of the principles equally. For example, the Individual Participation Principle (#8) may be of limited applicability in intelligence operations, as fusion centers do not generally engage with individuals. That said, fusion centers and all other integrated justice systems should endeavor to apply the FIPPs where practicable.

The eight principles are:

1) Purpose Specification
2) Data Quality/Integrity (see definition)
3) Collection Limitation/Data Minimization
4) Use Limitation
5) Security Safeguards (see definition)
6) Accountability/Audit
7) Openness/Transparency
8) Individual Participation

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.

Fusion Center - Fusion Center—Defined in the ISE-SAR Functional Standard, Version 1.5.5 as "[a] collaborative effort of two or more Federal, State, local, tribal, or territorial (SLTT) government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity." (Source: Section 511 of the 9/11 Commission Act). State and major urban area fusion centers serve as focal points within the State and local environment for the receipt, analysis, gathering, and sharing of threat-related information between the federal government and SLTT and private sector partners**.**

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

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

Data Quality - Data 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 Data Quality have been identified as accuracy, completeness, currency, reliability, and context/meaning. Today, Data 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.

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 Information Privacy.

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

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) Associated 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 U.S. Person 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.

Metadata – In its simplest form, metadata is information (data) about information, more specifically, information about a particular aspect of the collected information. An item of metadata may describe an individual content item or a collection of content items. Metadata is used to facilitate the understanding, use, and management of information. The metadata required for this will vary based on the type of information and the context of use.

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

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

Need to Know - 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 to perform or assist in a law enforcement, homeland security, or counterterrorism activity or other lawful and authorized government activity, such as to further an investigation or meet another law enforcement requirement.

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

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

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

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

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 gathered by a fusion center.

Participating Agency - An organizational entity that is authorized to access or receive and use center information and/or intelligence databases and resources for lawful purposes through its authorized individual users.

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

Privacy Impact Assessment (PIA) - is a process by which an entity can examine the P/CRCL risks in the entity's information system and sharing activities. In general, a PIA evaluates the process through which PII is collected, stored, protected, shared, managed, and purged. By completing a PIA, entities are able to identify P/CRCL vulnerabilities and to address and mitigate them through the design and implementation of policies. Ideally, PIAs are performed when information systems are created, and the results are used to inform the development of system P/CRCL policies. However, PIAs may also be completed when existing systems are significantly modified or at any time a system change creates P/CRCL risks. If the system is already operational, a PIA may still be conducted.

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.

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

U.S. Person – Per Executive Order 12333 "United States U.S. Person" means a United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, an unincorporated association substantially composed of individuals in the United States 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.

Pre-operational Planning – As defined in ISE-SAR Functional Standard, Version 1.5.5, "preoperational planning describes activities associated with a known or particular planned criminal operation or with terrorist operations generally."

Privacy - Privacy refers to individuals' interests in preventing the in appropriate gathering, 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.

P/CRCL Policy - A P/CRCL 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 gathering, analysis, maintenance, dissemination, and access. The purpose of the P/CRCL Policy is to articulate that the Center will adhere to those legal requirements and Center policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well-developed and implemented P/CRCL Policy uses justice entity resources wisely and effectively; protects the 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 gathering 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, which 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 - For the non-intelligence community, protected information is information about individuals in the United States and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and laws of the United States. For the (federal) intelligence community, protected information includes information about "United States U.S. Person" as defined in Executive Order 12333. Protected information may also include other information that the U.S. government expressly determines by Executive Order, international agreement, policy, or other similar instrument should be covered.
For state, local, tribal, and territorial governments, protected information may include information about individuals and organizations that is subject to information privacy or other legal protections by law, including the U.S. Constitution; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 23; applicable state and tribal constitutions; and applicable state, local, tribal, and territorial laws, ordinances, and codes. Protection may be extended to other individuals and organizations by fusion center or other state, local, tribal, or territorial agency policy or regulation.

Public - Public includes:

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

Public does not include:

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

Public Access - 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.

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

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

Record - Any item, collection, or grouping of information that includes PII and is collected, received, accessed, used, disseminated, retained, and purged by or for the collecting agency or organization.

Redress - Internal procedures to address complaints from U.S. Person regarding protected information about them that is under the Center's control.

Repudiation - The ability of a user to deny having performed an action those 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 – A requirement for access to specific information to perform or assist in a lawful and authorized governmental function. Right to know is determined by the mission and functions of a law enforcement, homeland security, counterterrorism, or other lawful and authorized

government activity or the roles and responsibilities of particular personnel in the course of their official duties.

Right to Information 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 Information 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.

Source Agency/Organization - Defined in the ISE-SAR Functional Standard, Version 1.5.5, source agency refers to the agency or entity that originates the SAR (examples include a local police department, a private security firm handling security for a power plant, and a security force at a military installation). The source organization will not change throughout the life of the SAR.

Storage

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- associated information, to include homeland security information, terrorism information, and law enforcement information relating to terrorism or the security of our homeland by both the originator of the information and any recipient of the information.

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

Suspicious Activity – Defined in the ISE-SAR Functional Standard, Version 1.5.5 as "oserved behavior reasonably indicative of preoperational planning associated with terrorism or other criminal activity." Examples of suspicious activity include surveillance, photography of sensitive infrastructure facilities, site breach or physical intrusion, cyberattacks, testing of security, etc.

Suspicious Activity Report (SAR) - Defined in the ISE-SAR Functional Standard, Version 1.5.5 as "official documentation of observed behavior reasonably indicative of preoperational planning associated with terrorism or other criminal activity." Suspicious activity report (SAR) information offers a standardized means for feeding information repositories or data analysis tools. Patterns identified during SAR information analysis may be investigated in coordination with the reporting agency and, if applicable, a state or regional fusion center. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor is it designed to support interagency calls for service.

Terrorism Information – Terrorism Information—Consistent with Section 1016(a)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), all information relating to (a) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or materials support, or activities of foreign or international terrorist groups or individuals or of domestic groups or individuals involved in transnational terrorism; (b) threats posed by such groups or individuals to the United States, United States persons, or United States interests or to those interests of other nations; (c) communications of or by such groups or individuals; or (d) other groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

Weapons of Mass Destruction (WMD) information was defined and included in the definition of "terrorism information" by P.L. 110-53.

Terrorism-Related Information—In accordance with the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended by the 9/11 Commission Act (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 the 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 may include intelligence information.

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

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

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

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

User – An individual representing a participating agency who is authorized to access or receive and use a center's information and intelligence databases and resources for lawful purposes.

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

Personnel Definitions

1) **Intelligence Personnel**
   A) All NDSLIC staff, analysts and field intelligence personnel (hereinafter referred to as intelligence personnel) are subject to the provisions of this P/CRCL Policy.
   B) Intelligence personnel include:
      i) **Criminal Intelligence Analysts -** Research, analyze and vet potential terrorism or criminal activity, suspect and incident data;
      ii) **Intelligence Supervisor** - First level of supervision over the NDSLIC Criminal Intelligence Analysts and products;
      iii) **Critical Infrastructure Program Manager/Physical Security Officer -** Research and analyze potential threats to critical infrastructure;
      iv) **State Law Enforcement Representatives -** Research, analyze, and bring intelligence to the NDSLIC from their respective parent organizations;
      v) **Local Law Enforcement Representatives -** Research, analyze, and bring intelligence to the NDSLIC from their respective parent organizations;
      vi) **Federal Law Enforcement Representatives -** Research, analyze, and bring intelligence to the NDSLIC 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 NDSLIC;

viii) **Federal Department of Homeland Security Intelligence and Analysis Representative -** Main conduit for classified Federal Department of Homeland Security information coming into the NDSLIC;

ix) **Director-** Handles NDSLIC day-to-day operations, organization, decision-making and quality control functions.

x) **NDNG Anti-Terrorism Program Specialist** - Act as Military Liaison with the NDSLIC - By researching, analyzing all potential threats to ND National Guard personnel, units, and facilities and disseminate that information as needed to the NDSLIC for situational awareness or for further action;

xi) **Information Systems Security Analyst** - Research, analyze, and bring intelligence to the NDSLIC from their respective parent organizations.

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 P/CRCL Policy.

C) Notwithstanding any other provisions of this P/CRCL 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 P/CRCL 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 P/CRCL Policy, authorized U.S. Person are Criminal Intelligence Analysts, Intelligence Supervisor, Infrastructure Program Manager , 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, Information Systems Security Analyst, Anti-Terrorism Program Specialist, the NDSLIC Director field intelligence personnel, public safety officials, certified law enforcement officers, and other criminal justice administrative personnel who:

i) Are approved for NDSLIC access by the NDSLIC Director, Chief of Operations, Chief of Administration, or Security Officer;

ii) Are approved for database access by BCI;

iii) Meet, at a minimum, the certification requirements for NDSLIC access; and

iv) Undergo training regarding the system's capabilities as well as the appropriate use and sharing of data accessed through the NDSLIC.

v) Receive a copy of this Policy and agree in writing to adherence of this Policy, by signing Appendix III.

5) **Authorized persons**

A) For purposes of this P/CRCL Policy, authorized persons are Criminal Intelligence Analysts, Intelligence Supervisor, 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 NDSLIC Director , field intelligence personnel, public safety officials, certified law enforcement officers, and other criminal justice administrative personnel in the furtherance of their official duties.

B) The information has been provided on a need to know basis and will be afforded the proper security at all times. This information shall not be released to any non-criminal justice agency or person. This information may be protected under state law (N.D.C.C. Section 44-04-18.7) or applicable federal laws and may be withheld.

Information

1) **The NDSLIC will seek or retain information (including "protected attributes") subject to conditions articulated that:**

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

2) In accordance with applicable laws, guidance, and regulations, the NDSLIC will not seek or retain and will inform information-originating agencies not to submit information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, national origin, ages, disabilities, genders, gender identities, or sexual orientations. When participating on a federal law enforcement task force or when documenting a SAR or an ISE-SAR in the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI), race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity must not be considered as factors creating suspicion. However, those attributes may be documented in specific suspect descriptions for identification purposes.

3) The NDSLIC may retain protected information that is based on a level of suspicion that is "reasonable suspicion" and/ or is "reasonably indicative" 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 and North Dakota Century Code (N.D.C.C.) Chapter 54-46 (North Dakota Record Management Program). In addition, NDSLIC may require a contributing agency to justify why any particular tip, lead, intelligence report should remain in the system if it appears to NDSLIC personnel that the information is no longer active or otherwise of intelligence or investigative value. Failure to satisfy NDSLIC's request may result in the information being unilaterally removed from the intelligence database system. Notice of any such removal may be made to the contributor by the Privacy Officer.

4) The NDSLIC 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 restricting access, use, or disclosure.

5) The NDSLIC will identify and review protected information that may be accessed from or disseminated by the Center prior to sharing that information through the ISE. 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 NDSLIC 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- associated 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 gathered 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 NDSLIC submission standards.
   D) Any particular limitations to the use or disclosure of the information.

7) The NDSLIC 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 NDSLIC will, upon receipt of information, review the information to determine its nature and purpose. Once information is reviewed at the NDSLIC, NDSLIC 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) Unreliable - the reliability of the source is doubtful or has been determined to be unreliable
      iii) 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 NDSLIC personnel in determining source reliability and content validity. NDSLIC personnel may reject information as failing to meet any criteria (i.e. reasonable suspicion) for inclusion and return such information to the submitting party with an indication of why it was rejected. Information not meeting the criminal intelligence standard may be entered into NDSLIC’s Tips and Leads Database.
   G) Tips and Leads determined to be non-validated will be purged from the intelligence database 3 years from the date of submission.

9) At the time a decision is made to contribute information into the intelligence database, NDSLIC 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) NDSLIC 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 gathering 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 NDSLIC 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 per the NDSLIC’s Records Retention Schedule to analyze a tip or lead to determine its credibility and value, (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.
    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 gathered, 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 1.5.5) and align with Part B of the ISE-SAR Functional Standard (the need for additional fact development during the vetting process under certain circumstances).

14) The NDSLIC will keep a record of the originating entity for all information gathered by the Center.

Acquiring and Receiving Information

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

   A) The NDSLIC intelligence personnel will comply with Information Sharing Environment Guidelines and will follow 28 CFR Part 23 with regard to criminal 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 ISE.

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 NDSLIC. If the NDSLIC is notified or otherwise learns that information has been obtained illegally, the information will be removed.

3) Agencies which utilize the NDSLIC 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 NDSLIC 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 gathering practices.

4) The NDSLIC 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.

Data Quality and Assurance

The NDSLIC 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 criminal intelligence information retained by the NDSLIC must be 28 CFR Part 23 and 28 CFR Part 20 compliant.

1) **Data Labeling**

At the time of retention in the system NDSLIC 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. 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 NDSLIC's intelligence database; to include tips and leads are considered the property of the NDSLIC and BCI.

3) **Data Accuracy**

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

D) The NDSLIC 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 NDSLIC 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.

i) The following NDSLIC Staff members are authorized to merge records;
   (1) Director
   (2) Privacy Officer
   (3) Intelligence Supervisor
   (4) Criminal Intelligence Analysts

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 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.[9]

[9] As required by 28 CFR Part 23.20(h) and 28 CFR Part 20

B) Inaccurate information can have a damaging impact upon the data subject and the integrity and functional value of NDSLIC query responses. Any information obtained through a query to the NDSLIC 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 NDSLIC Privacy and Policy Committee is responsible for monitoring the use of all NDSLIC data sources to guard against inappropriate or unauthorized use.

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

C) All NDSLIC inquiries by authorized U.S. Person will be made available, upon request, to that authorized person's agency.

D) ND BCI will ensure and maintain the integrity of NDSLIC intelligence database in compliance with 28 CFR Part 23, 28 CFR Part 20 and NDSLIC record retention policy.

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

F) Random audits are performed on a continual basis and at least once a year by BCI appointed personnel and NDSLIC Privacy Officer. When information is found to be erroneous or deficient by either the BCI or NDSLIC Privacy Officer, such that an individual's privacy rights are impacted, the BCI appointed personnel and NDSLIC Privacy Officer's responsibilities are limited to notifying the original source agency in writing for their follow-up and correction.[10]

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

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

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

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;

[10] 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 P/CRCL Policy.

a) All re-disclosure or secondary dissemination by the NDSLIC must be logged in accordance with the Sharing and Disclosure Section of this P/CRCL Policy.

b) External agencies which have received NDSLIC 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 NDSLIC.

Data Collation Standards

1) Information acquired or received by the NDSLIC 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 Data Quality and Information Assurance sections of this Policy.
3) Information acquired or received by the NDSLIC 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 NDSLIC.

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 NDSLIC Director has assigned the Privacy Officer and other designees' oversight responsibility to review NDSLIC products prior to dissemination by the center to protect privacy, civil rights, and civil liberties.
5) The NDSLIC incorporates the gathering, processing, reporting, analyzing, and sharing of terrorism- associated 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 NDSLIC intelligence personnel may receive information that is based on a level of suspicion that is less than "reasonable indicative" 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 gathered in an authorized and lawful manner 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 associated 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 NDSLIC'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 gathering codes and a sharing process that complies with the ISE-SAR Functional Standard for suspicious activity potentially associated to terrorism.
3) Access or disclosure of records retained by the NDSLIC will be provided only to personnel within the NDSLIC 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 NDSLIC 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 NDSLIC 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 and records retained by the NDSLIC 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 applicable state or federal 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 SAR Data Repository by the NDSLIC 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 NDSLIC mission and is not exempt from disclosure by applicable state or federal law.

9) NDSLIC 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): § 44-04-18.4 (7) (Security and Cyber Attacks); § 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); § 44-04-18.10(6) (Emergency Planning and Response);§ 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); § 44-04-24 (Critical Infrastructure and Security Planning, Mitigation, or Threats); § 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); 18 U.S.C. 113B (Terrorism).

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 Pre-assessment 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); § 44-04-18.4(7) (Confidentiality of trade secret, proprietary, commercial, financial, and research information.);§ 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 NDSLIC 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.

D) Federal Laws, Regulations, and Guidance

i) Brady Handgun Violence Prevention Act, 18 U.S.C. §§ 921, 922, 924, and 925A, United States Code, Title 18, Part I, Chapter 44, §§ 921, 922, 924, and 925A—The Brady Act, passed in 1993, requires background checks for purchases of firearms from federally licensed sellers. Because the act prohibits transfer of a firearm to a person who is prohibited by law from possessing a firearm, the transmission of personal data is an integral part of the regulation.

ii) Computer Matching and Privacy Act of 1988, 5 U.S.C. § 552a(a), United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a(a); see also Office of Management and Budget (OMB), Memorandum M-01-05, "Guidance on Interagency Sharing of Personal Data—Protecting Personal Privacy," December 20, 2000—The Computer Matching and Privacy Act of 1988 (Matching Act) amended the Privacy Act of 1974 to require that data-matching activities or programs of federal agencies that are designed to establish or verify eligibility for federal benefit programs or for recouping payments for debts under covered programs protect personal information. This is accomplished through a computer matching agreement and publication of a notice in the Federal Register. The OMB guidance requires that interagency data sharing provide protection, including provisions for notice, consent (as appropriate), redisclosure limitations, accuracy, security controls, minimization, accountability, and use of Privacy Impact Assessments. Although not directly a requirement of state, local, tribal, and territorial (SLTT) agencies, the guidance is a useful source of information on the types of protections that should be considered for all interagency data sharing programs.

iii) Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFR Part 2, Code of Federal Regulations, Title 42: Public Health, Part 2-42 CFR Part 2 establishes minimum standards to govern the sharing of substance abuse treatment records (patient history information) in programs that are federally assisted. Generally, the sharing of such information is limited to the minimum necessary for the allowed purpose and requires consent of the patient except in specific emergency situations, pursuant to a court order or as otherwise specified. State law should also be consulted to determine whether there are additional limitations or sharing requirements.

iv) Confidentiality of Identifiable Research and Statistical Information, 28 CFR Part 22, Code of Federal Regulations, Title 28, Chapter I, Part 22-28 CFR Part 22 is designed to protect the privacy of individuals whose personal information is made available for use in a research or statistical program funded under the Omnibus Crime Control and Safe Streets Act of 1968, the Juvenile Justice and Delinquency Prevention Act of 1974, or the Victim of Crimes Act. The regulation, which may apply to SLTT agencies that conduct research or statistical programs, limits the use of such information to research or statistical purposes; limits its revelation to a need to know basis; provides for final disposition, transfer, and notice to/consent of data subjects; and identifies sanctions for violations. It provides useful guidance for SLTT agencies that wish to make data containing personal information available for research or statistical purposes.

v) Crime Identification Technology, 42 U.S.C. § 14601, United States Code, Title 42, Chapter 140, Subchapter I, § 14601—This statute authorizes the Office of Justice Programs (OJP), U.S. Department of Justice (D0J), to support technological advances by states directed at a variety of criminal justice purposes, such as identification of certain categories of offenders, conducting background checks, and determining eligibility for firearms possession. The act defines broad categories of

purposes for which funds may be used by OJP and sets forth certain eligibility criteria and assurances and other protocols that must be followed.

vi) Criminal History Records Exchanged for Noncriminal Justice Purposes, 42 U.S.C. § 14611, United States Code, Title 42, Chapter 140, Subchapter II, § 14611—This statute provides a general overview of the Interstate Identification Index System (IIIS), an information sharing system that contains state and federal criminal history records that are also used for non-criminal justice purposes, such as governmental licensing and employment background checks. Congress recommends the creation of interstate and federal-state agreements to ensure that uniform policies are in place for records exchanges for non-criminal justice purposes and to prevent unauthorized use and disclosure of personal information due to variances in authorized users' policies. This statute is applicable to multijurisdictional information sharing systems that allow non-criminal justice-related exchanges.

vii) Criminal Intelligence Systems Operating Policies, 28 CFR Part 23, Code of Federal Regulations, Title 28, Chapter 1, Part 23—This is a guideline for law enforcement agencies that operate federally funded multijurisdictional criminal intelligence systems. The operating principles of 28 CFR Part 23 provide guidance to law enforcement regarding how to operate criminal intelligence information systems effectively while safeguarding privacy, civil rights, and civil liberties during the collection, storage, and dissemination of criminal intelligence information. The regulation governs the intelligence information systems' process, which includes information submission or collection, secure storage, inquiry and search capability, controlled dissemination, and review and purge processes.

viii) Criminal Justice Information Systems, 28 CFR Part 20, Code of Federal Regulations, Title 28, Chapter 1, Part 20—This applies to all state and local agencies and individuals collecting, storing, or disseminating criminal history record information processed by manual or automated operations and funded by the Omnibus Crime Control and Safe Streets Act of 1968, codified at 42 U.S.C. § 3789D. The regulation requires those criminal justice information systems to submit a criminal history information plan and provides guidance on specific areas that should have a set of operational procedures. These areas include completeness and accuracy of criminal history records and limitations on dissemination, including general policies on use and dissemination, juvenile records, audits, security, and access and review.

ix) Disposal of Consumer Report Information and Records, 16 CFR Part 682, Code of Federal Regulations, Title 16, Chapter I, Part 682-16 CFR Part 682 applies to information systems that maintain or possess consumer information for business purposes. The regulation provides guidance on proper disposal procedures for consumer information records to help protect against unauthorized use or access.

x) Driver's Privacy Protection Act of 1994, 18 U.S.C. 2721—Prohibition on Release and Use of Certain Personal Information from State Motor Vehicle Records—Collected License Plate Reader (LPR) information contains no Pll that may be used to connect a license plate detection to an individual. It is only with permissible purpose that law enforcement may make this connect (using other systems), and this access is governed by the Driver's Privacy Protection Act of 1994. www.gpo.gov/fdsys/granule/USCODE-2011-title18/USCODE-2011-title18-oartlchao123-sec2721/content-detail.html

xi) E-Government Act of 2002, Pub. L. No. 107-347, 208, 116 Stat. 2899 (2002); OMB (03-22, OMB Memorandum, M-03-22, OMB Guidance for Implementing the Privacy

Provisions of the E-Government Act of 2002)-0MB implementing guidance for this act requires federal agencies to perform Privacy Impact Assessments (PIA) for new information technologies that develop or procure new information technology involving the collection, maintenance, or dissemination of information in identifiable form or that make significant changes to existing information technology that manages information in identifiable form. A PIA is an evaluation of how information in identifiable form is collected, stored, protected, shared, and managed. The purpose of a PIA is to demonstrate that system owners and developers have incorporated privacy, civil rights, and civil liberties protections throughout the entire life cycle of a system. The act requires an agency to make PIAs publicly available, except when an agency in its discretion determines publication of the PIA would raise security concerns or reveal classified (i.e., national security) information or sensitive. Although this act does not apply to SLTT partners, this tool is useful for identifying and mitigating privacy risks and for notifying the public what Pit the SLTT agency is collecting, why Pit is being collected, and how the Pit will be collected, used, accessed, shared, safeguarded, and stored.

xii) Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2522, 2701-2709, United States Code, Title 18, Part I, Chapter 119, §§ 2510-2522, 2701-2709, and 3121-3125, Public Law 99-508—This set of statutes prohibits a person from intentionally intercepting, trying to intercept, or asking another person to intercept or try to intercept any wire, oral, or electronic communication or trying to use information obtained in this manner. From another perspective, the law describes what law enforcement may do to intercept communications and how an organization may draft its acceptable use policies and monitor communications. Although it is a federal statute, the act does apply to state and local agencies and officials.

xiii) Fair Credit Reporting Act, 15 U.S.C. § 1681, United States Code, Title 15, Chapter 41, Subchapter III, § 1681—The Fair Credit Reporting Act regulates the collection, dissemination, and use of consumer information, including consumer credit information by consumer reporting agencies. Consumer reporting agencies include specialty agencies, such as agencies that sell information about employment history, insurance claims, check-writing histories, medical records, and rental history records, as well as credit bureaus. The law primarily deals with the rights of people about whom information has been gathered by consumer reporting agencies and the obligations of the agencies. Government agencies may obtain information from these reporting agencies and should be aware of the nature and limitations of the information, in terms of collection, retention, and error correction.

xiv) Federal Civil Rights Laws, 42 U.S.C. § 1983, United States Code, Title 42, Chapter 21, Subchapter I, § 1983—This is a federal statute that allows an individual to sue public officials in federal court for violations of the individual's civil rights. Civil rights include such things as the Fourth Amendment's prohibitions against unreasonable search and seizure, violations of privacy rights, and violations of the right to freedom of religion, free speech, and free association. It serves as a deterrent to unlawful collection, use, or sharing of information rather than providing specific authority or a prohibition to the collection, use, or sharing of information.

xv) Federal Driver's Privacy Protection Act (DPPA), 18 USC § 2721-2725—Restricts access and prohibits the release of personal information from state motor vehicle records to ensure the privacy of persons whose records have been obtained by that department in connection with a motor vehicle record unless certain criteria are met.

xvi) Federal Records Act, 44 U.S.C. § 3301, United States Code, Title 44, Chapter 33, § 3301—This chapter contains the laws governing disposal of records made or received by a federal agency in the normal course of business. It discusses procedures and notices, if required, and the role of the federal archivist. The law applies only to federal agencies, but there may be similar state or local laws applicable to state and local agencies.

xvii) Freedom of Information Act (FOIA), 5 U.S.C. § 552, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552—The federal FOIA, enacted in 1966, provides access to federal agency records or information. It does not, however, allow access to state or local government records. Nearly all states have their own public access statutes that provide access to state- and local-agency records. The interaction of federal and state FOIA laws can create complex issues. Federal statutes, in essence, provide a baseline of legal protections for individuals. While state legislatures may pass laws to supplement these federal guidelines, state laws that interfere with or are contrary to a federal law are preempted. By virtue of the Supremacy Clause of the U.S. Constitution (Article VI, Clause 2), federal law may restrict access to records otherwise available pursuant to a state's FOIA by requiring that certain information be kept confidential. Thus, federal confidentiality requirements may supersede a state FOIA statute mandating public disclosure of a record, but only when there is a specific federal statute (other than the federal FOIA) that mandates the records be kept confidential. In short, records may be available under one FOIA statute but not pursuant to another.

xviii) Health Insurance Portability and Accountability Act (HIPAA) of 1996,42 U.S.C. § 201, United States Code, Title 42, Chapter 6A, Subchapter I, § 201; Public Law 104-191—HIPAA was enacted to improve the Medicare and Medicaid programs and the efficiency and effectiveness of the nation's health care system by encouraging the development of a national health information system through the establishment of standards and requirements for the electronic transmission of health information. To that end, Congress directed the U.S. Department of Health and Human Services (HHS) to issue safeguards to protect the security and confidentiality of health information. To implement HIPAA's privacy requirements, HHS promulgated regulations setting national privacy standards for health information: the Standards for Privacy of Individually Identifiable Health Information (the "Privacy Rule")-42 U.S.C. §1320d-2; 45 CFR Parts 160, 164 (2003).

xix) HIPAA, Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164, Code of Federal Regulations, Title 45, Parts 160 and 164—This "Privacy Rule" sets forth national standards for the privacy and security of individually identifiable health information (45 CFR Part 164, Subpart E (2003)). This rule has been described as providing a "federal floor" of safeguards to protect the confidentiality of medical information. State laws that provide stronger privacy protection will continue to apply over and above the federal privacy protection. The general rule under these standards states that a covered entity may not use or disclose protected health information except as permitted or required by the rules (45 CFR Part 164.502(a) and §164.103 [defining protected health information and use]). The Privacy Rule applies to the following covered entities: (1) a health plan, (2) a health care clearinghouse, and (3) a health care provider who transmits any health information in electronic form in connection with certain transactions (42 U.S.C. §1320d-1(a) (2003); 45 CFR Part 160.102 (2003). Since the Privacy Rule applies only to a covered entity, a governmental body begins its inquiry by first determining

whether it is a covered entity under the Privacy Rule (45 CFR Part 160.103 (2003) [defining health plan, health care clearinghouse, health care provider]). If it is a covered entity, it then looks to the Privacy Rule for a permitted or required disclosure.

xx) Indian Civil Rights Act of 1968, 25 U.S.C. § 1301 et seq., United States Code, Title 25, Chapter 15, Subchapter I—This act contains definitions of relevant terms and extends certain constitutional rights to Indian tribes exercising powers of self-government.

xxi) Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Section 1016, as amended by the 9/11 Commission Act—This act broadly affects U.S. terrorism law and applies directly to the federal government. It establishes the Director of National Intelligence, the National Counterterrorism Center, and the Privacy and Civil Liberties Oversight Board. Of importance to SLTT agencies, IRTPA establishes the Information Sharing Environment (ISE) (see Appendix A, Glossary of Terms and Definitions) for the sharing of terrorism-related information at all levels of government, with private agencies, and with foreign partners.

xxii) National Child Protection Act of 1993, Public Law 103-209 (December 20, 1993), 107 Stat. 2490—In each state, an authorized criminal justice agency of the state shall report child abuse crime information to or index child abuse crime information in the national criminal history background check system. A criminal justice agency can satisfy the requirement by reporting or indexing all felony and serious misdemeanor arrests and dispositions. The U.S. Attorney General (AG) is required to publish an annual statistical summary of child abuse crimes. The act requires that 80 percent of final dispositions be entered in the state databases by December 1998, with steps being taken toward 100 percent entry. A 1994 amendment required that the AG—in consultation with federal, state, and local officials, including officials responsible for criminal history record systems, and representatives of public and private care organizations and health, legal, and social welfare organizations—shall develop guidelines for the adoption of appropriate safeguards by care providers and by the state for protecting children, the elderly, and individuals with disabilities from abuse.

xxiii) National Crime Prevention and Privacy Compact, 42 U.S.C. § 14616, United States Code, Title 42, Chapter 140, Subchapter II, § 14616—The compact establishes an infrastructure by which states can exchange criminal records for non-criminal justice purposes according to the laws of the requesting state and provide reciprocity among the states to share records without charging each other for the information. The Compact Council, as a national independent authority, works in partnership with criminal history record custodians, end users, and policymakers to regulate and facilitate the sharing of complete, accurate, and timely criminal history record information to noncriminal justice users in order to enhance public safety, welfare, and the security of society while recognizing the importance of individual privacy rights.

xxiv) National Security Act, Public Law 235, Section 606, in accordance with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010—The National Security Act of 1947 mandated a major reorganization of foreign policy and military establishments of the U.S. government. The act created many of the institutions that U.S. Presidents found useful when formulating and implementing foreign policy, including the National Security Council and the Central Intelligence Agency. The 1947 law also caused far-reaching changes in the military establishment. The War Department and

Navy Department merged into a single U.S. Department of Defense under the Secretary of Defense, who also directed the newly created Department of the Air Force. However, each of the three branches maintained its own service secretaries.

xxv) On October 7, 2011, President Barack Obama signed Executive Order 13549, entitled, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information." This order directs structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks that shall be consistent with appropriate protections for privacy and civil liberties. Agencies bear the primary responsibility for meeting these twin goals. These structural reforms will ensure coordinated interagency development and reliable implementation of policies and minimum standards regarding information security, personnel security, and systems security; address both internal and external security threats and vulnerabilities; and provide policies and minimum standards for sharing classified information both within and outside the federal government. These policies and minimum standards will address all agencies that operate or access classified computer networks, all users of classified computer networks (including contractors and others who operate or access classified computer networks controlled by the federal government), and all classified information on those networks.

xxvi) NIST Special Publication 800-53 (Appendix J) Security and Privacy Controls for Federal Information Systems and Organizations—Federal agencies are required to ensure that privacy protections are incorporated into information security planning. To that end, SP 800-53 Rev. 4 features eight families of privacy controls that are based on the FIPPs. The proliferation of social media, Smart Grid, mobile, and cloud computing as well as the transition from structured to unstructured information and metadata environments have added significant complexities and challenges for federal organizations in safeguarding privacy. These challenges extend well beyond the traditional information technology security view of protecting privacy, which focused primarily on ensuring confidentiality. The use of these standardized privacy controls will provide a more disciplined and structured approach for satisfying federal privacy requirements and demonstrating compliance with those requirements. Like their federal partners, SLTT agencies may use the privacy controls when evaluating their systems, processes, and programs.

xxvii) Preparing for and Responding to a Breach of Personally Identifiable Information, OMB Memorandum M-17-12 (January 2017)—This memorandum sets forth the policy for federal agencies to prepare for and respond to a breach of PII. It includes a framework for assessing and mitigating the risk of harm to individuals potentially affected by a breach, as well as guidance on whether and how to provide notification and services to those individuals. This memorandum is intended to promote consistency in the way agencies prepare for and respond to a breach by requiring common standards and processes.

xxviii) Privacy Act of 1974, 5 U.S.C. § 552a, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a—The Privacy Act establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual. The Privacy Act prohibits the disclosure of a record about an individual from a system of records absent the written consent of the individual,

unless the disclosure is pursuant to one of twelve statutory exceptions. The act also provides individuals with a means by which to seek access to and amendment of their records and sets agency recordkeeping requirements. In addition, the Privacy Act requires that agencies give the public notice of their systems of records by publication in the Federal Register.

xxix) Privacy of Consumer Financial Information, 16 CFR Part 313, Code of Federal Regulations, Title 16, Chapter I, Part 313—This code oversees the treatment of nonpublic personal information about consumers by financial institutions and requires the institution to provide notice to customers about its privacy policies, the conditions under which it can disclose this information, and its opt out policies. This code also prohibits the disclosure of a consumer's credit card, deposit, or transaction account information to nonaffiliated third parties to market to the customer. The requirements for initial notice for the "opt-out" do not apply when nonpublic personal information is disclosed in order to comply with federal, state, or local laws or to comply with an authorized investigation, subpoena, or summons.

xxx) Protection of Sensitive Agency Information, Office of Management and Budget Memorandum M-06-16 (June 2006)—This memorandum provides a security checklist from the National Institute of Standards and Technology (NIST) to protect remote information removed from or accessed from outside an agency's physical location specific to PII. The NIST checklist requires that agencies verify Pll in need of protection, confirm the adequacy of organization policy surrounding Pll protection, and implement any necessary protections for Pll transported or stored off-site or accessed remotely. In addition to the NIST checklist, the memorandum recommends implementing information encryption on all mobile devices, allowing remote access only with two factor authentication, using timeout functions on devices, and logging all computer-readable information extracts from databases with sensitive information, while verifying that each extract has either been erased within 90 days or that its use is still required.

xxxi) Safeguarding Customer Information, 16 CFR Part 314, Code of Federal Regulations, Title 16, Chapter I, Part 314—This Federal Trade Commission regulation implements Sections 501 and 505(b)(2) of the Gramm-Leach-Bliley Act. It sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information by financial institutions. While not directly applicable to government agencies, the regulation is useful in outlining the elements of a comprehensive information security program, including administrative, technical, and physical safeguards designed to (1) ensure the security and confidentiality of information, (2) protect against any anticipated threats or hazards to the security or integrity of information, and (3) protect against unauthorized access to or use of information that could result in substantial harm or inconvenience to any individual.

xxxii) Sarbanes-Oxley Act of 2002, 15 U.S.C., Chapter 98, § 7201, United States Code, Title 15, Chapter 98, §7201—The Sarbanes-Oxley Act of 2002, Pub. L. 107-204 (July 30, 2002), commonly called Sarbanes-Oxley, is a federal law that sets new or enhanced standards for all U.S. public company boards, management, and public accounting firms. Its 11 titles include standards for public audits, internal controls, and financial disclosure. While not applicable to federal, state, local, tribal, or territorial governmental agencies, the business standards established by Sarbanes-

Oxley are of value to such agencies in establishing their own policies and procedures to guide and control their business processes.

xxxiii) Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Public Law 107-56 (October 26, 2001), 115 Stat. 272—The USA PATRIOT Act was enacted in response to the terrorist attacks on September 11, 2001. The act was designed to reduce the restrictions on law enforcement agencies' ability to gather intelligence and investigate terrorism within the United States; expand the Secretary of the Treasury's authority to regulate financial transactions, particularly those involving foreign individuals and entities; and broaden the discretion of law enforcement and immigration authorities in detaining and deporting illegal immigrants suspected of terrorism-related acts. The act also expanded the definition of "terrorism" to include domestic terrorism. In 2011, the act was extended for four years, including provisions for roving wiretaps, searches of business records, and the conduct of surveillance of "lone wolves"—individuals suspected of terrorism related activities that are not linked to terrorist groups.

xxxiv) U.S. Constitution, First, Fourth, Fifth, Sixth, and Fourteenth Amendments—The Bill of Rights establishes minimum standards for the protection of the civil rights and civil liberties of individuals in the United States. The First Amendment protects religious freedom, speech, the press, the right to peaceably assemble, and the right to petition the government for a redress of grievances. The Fourth Amendment protects the people from unreasonable searches and seizures and requires that warrants be issued only upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the individual or things to be seized. The Sixth Amendment establishes the right of an accused individual to a speedy and public trial by an impartial jury, to be informed of the nature and cause of the charges, to confront witnesses, to have compulsory process to obtain witnesses, and to have the assistance of legal counsel. The Fourteenth Amendment addresses citizenship rights and equal protection of the laws. Although the equal protection clause applies explicitly only to state governments, equal protection requirements apply to the federal government through the Fifth Amendment Due Process Clause.

xxxv) The USA FREEDOM Act of 2015 extended some provisions of the USA PATRIOT Act addressing the tracking of "lone wolves" and "roving wiretaps" of targets that communicate through multiple devices and replacing provisions related to "bulk collection" under Section 215 of the Patriot Act, with a requirement for a specific selection term used to limit the scope of tangible things sought consistent with the purpose for seeking those things in addition to showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.

xxxvi) Applicants and Recipients of Immigration Relief Under the Violence Against Women Act of 1994 (VAWA), Public Law 103-322, September 13, 1994, and the Victims of Trafficking and Violence Prevention Act of 2000 (T and U nonimmigrant status for victims of trafficking and other serious crimes), Public Law 106-386, Oct. 28, 2000, 8 U.S.C. § 1367, Penalties for Disclosure of Information—The governing statute prohibits the unauthorized disclosure of information about VAWA, T, and U cases to anyone other than an officer or employee of the U.S. Department of Homeland Security, the U.S. Department of Justice, the U.S. Department of State, or

parties covered by exception when there is a need to know. This confidentiality provision is commonly referred to as "Section 384" because it originally became law under Section 384 of the Illegal Immigration Reform and Immigrant Responsibility Act (IIRIRA) of 1996, [5] which protects the confidentiality of victims of domestic violence, trafficking, and other crimes who have filed for or have been granted immigration relief. 8 U.S.C. § 1367 Information is defined as any information relating to aliens who are seeking or have been approved for nonimmigrant or immigrant status as (1) battered spouses, children, or parents under provisions of VAWA; (2) victims of a severe form of human trafficking who generally are cooperating with law enforcement authorities (nonimmigrant status); or (3) aliens who have suffered substantial physical or mental abuse as the result of qualifying criminal activity and have been, are being, or are likely to be helpful in the investigation or prosecution of that activity (nonimmigrant status). This includes information pertaining to qualifying family members who receive derivative T, U, or VAWA status. Because 8 U.S.C. § 1367 applies to any information about a protected individual, this includes records or other information that do not specifically identify the individual as an applicant for or a beneficiary of T nonimmigrant status, U nonimmigrant status, or relief under VAWA.

Redress

1) Information that is retained by the NDSLIC, 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 Department of Emergency Services; NDDESRECORDS@nd.gov. 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 NDSLIC. 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:

   - The disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution[11];

[11] 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.

- The disclosure would endanger the health or safety of an individual, organization, or community[12];
- The information is in a criminal intelligence system[13].

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 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 NDSLIC 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 NDSLIC 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 NDSLIC 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- associated protected information that:

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

   C) The NDSLIC will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the NDSLIC's Privacy Officer at the following: ndslic@nd.gov or 701-328-8172. 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

---

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

[13] 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; 18 U.S.C. 113B (Terrorism) .

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 NDSLIC 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 NDSLIC, the NDSLIC**,** 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 NDSLIC 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 SAR Data Repository 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 NDSLIC maintains records of agencies sharing terrorism- associated 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 directors sit on the NDSLIC Executive Board, have Information Security Officers who support the NDSLIC and are trained to handle network access/security and manage firewalls that are in place to prevent unauthorized agencies or entities from accessing NDSLIC resources.

2) The NDSLIC 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 NDSLIC 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 NDSLIC 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 NDSLIC data outlined at their respective agencies.

4) The NDSLIC will adhere to and follow the NDSLIC 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 NDSLIC Executive Board has appointed the ND Critical Infrastructure Program Manager as the NDSLIC Physical Security Officer. Operation security, site security, and information security training, including the handling of classified information, and derivative classifications, is provided to the 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 NDSLIC personnel become aware of a breach of the security of unencrypted personal information, The NDSLIC Privacy Officer will determine whether the center's response can be conducted at the staff level or whether a breach response team, consisting of the Privacy Officer, Director, the center's security officer, legal counsel, privacy oversight committee, and/or other designee(s) will be convened to respond to the breach. The Privacy Officer, in coordination with the breach response team, when applicable, will assess the risk of harm to individuals potentially affected by a breach (i.e., the nature and sensitivity of the PII potentially compromised by the breach, the likelihood of access and use of PII, and the type of breach involved), evaluate how the center may best mitigate the identified risks, and provide recommendations to the Director on suggested countermeasures, guidance, or other actions. 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 NDSLIC 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- associated information shared through the ISE-SAR. The database log/audit trail automatically captures the NDSLIC user. The NDSLIC user must manually enter the requesting/submitting agency and officer's name. Audit log/trail or dissemination records are stored in the NDSLIC intelligence database.

9) Risk, consequence, and vulnerability assessments maybe stored separately from law enforcement, intelligence, and public data. Risk, consequence 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 the NDSLIC as provided by 28 CFR Part 23 and NDSLIC record retention policy.

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

   A) NDSLIC intelligence databases will automatically audit data that has met the five-year retention period (28 CFR Part 23 standard) and NDSLIC record retention policy. Data that has not been validated is purged.
   B) If the information has not been updated and/or validated, it will be removed from the system at the end of the retention period. Material purged from the intelligence system shall be destroyed.[14]
   C) Non-intelligence information will be maintained and/or destroyed in accordance with the NDSLIC record retention policy.
   D) No confirmation of deleted information will be provided

3) 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 NDSLIC is destroyed or returned in accordance with this policy or as otherwise agreed upon with the originating agency.
4) Notification of proposed destruction or return of records may or may not be provided to the originating agency by the NDSLIC, depending on the relevance of the information and any agreement with the originating agency.
5) The NDSLIC 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 maybe given to the submitter at least 30 days prior to the required review and validation/purge date.
6) 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.

   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 NDSLIC is destroyed or returned in accordance with this policy or as otherwise agreed upon with the originating agency.

[14] Electronic records are permanently purged and paper files are shredded.

7) 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

Accountability and Enforcement

1) Information System Transparency

   A) The approved P/CRCL Policy will be displayed for general view on the NDSLIC website at https://www.ndslic.nd.gov/ . Intelligence personnel and agencies with access to NDSLIC 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 NDSLIC Privacy Officer. The Privacy Officer can be contacted at: ndslic@nd.gov or 701-328-8172.

2) Accountability

   A) All intelligence personnel are required to abide by this P/CRCL Policy and applicable laws which govern the treatment of the information the NDSLIC gathers, receives, maintains, archives, accesses, or discloses.

   B) User Compliance

      i) The NDSLIC P/CRCL Policy Committee is responsible for monitoring the use of all NDSLIC data sources to guard against inappropriate or unauthorized use.

      ii) The NDSLIC P/CRCL Policy Committee will investigate misuse of NDSLIC data and conduct or coordinate audits with the BCI concerning the proper use and security of NDSLIC data.

         (1) All entries of new NDSLIC intelligence database users are reviewed by the NDSLIC Privacy and Policy Committee for the first 60 days.

         (2) The NDSLIC Privacy and Policy Committee will randomly review 1% percent of all NDSLIC intelligence database entries annually.

   C) Violations

      i) When the NDSLIC Privacy and Policy Committee learn of a violation of policy, laws, or regulations concerning the use of NDSLIC data, it must notify the chief executive of the offending agency in writing. Agencies must act to correct such violations and

provide an assurance in writing to the NDSLIC Director or Privacy Officer that corrective action has been taken.

ii) Any suspected or documented misuse of NDSLIC information discovered by or reported to a law enforcement agency must be reported by that agency to the NDSLIC Privacy Officer.

D) The NDSLIC P/CRCL Policy and all Standard Operating Procedures (SOPs) are reviewed by the NDSLIC Director, Chief of Operations or Privacy Officer 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 P/CRCL Policy regarding the gathering, use, retention, destruction, sharing, classification, or disclosure of information, the NDSLIC 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 NDSLIC 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 P/CRCL Policy.

Training

1) The NDSLIC abides by the Bureau of Justice Assistance (BJA) 28 CFR Part 23 online training as the education and training standard annually for all NDSLIC personnel.

A) Training is provided annually on the P/CRCL Policy to all intelligence personnel.

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

C) The NDSLIC will provide special training regarding the Center's requirements, policies for gathering, use, and disclosure of protected information to personnel authorized to share protected information through the ISE.

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

E) Private sector personnel engaged in a partnership with the NDSLIC will receive training on this P/CRCL Policy.

2) The NDSLIC's annual P/CRCL Policy training program will cover:

A) How to protect P/CRCL throughout the fusion process, including handling, receipt, analysis, gathering, and dissemination of information and intelligence

B) Understanding potential P/CRCL issues and the ISE-SAR vetting process

a. ISE Core Awareness Training

b. Handling RFIs

c. Common errors with P/CRCL implications in preparing intelligence products
d. Countering Violent Extremism (CVE) (incorporating the White House's Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism)
e. Cultural awareness
f. Safeguarding personally identifiable information (PII)
g. Hot topics/current issues (e.g., mental health databases/release of information)

Appendix I

Yearly Revision Annex 2018 – 2019 **Revision Date: 06/26/2019**

Available Upon Request