NEW HAMPSHIRE

Information and Analysis Center

NH Information and Analysis Center

Privacy, Civil Rights, and Civil Liberties Policy

Effective Date: December 2014

Revised 25 January 2021

A. Purpose Statement 3
B. Policy Applicability and Legal Compliance 3
C. Governance and Oversight 4
D. Definitions 5
E. Information 5
F. Acquiring and Receiving Information 8
G. Information Quality Assurance 9
H. Collation and Analysis 10
I. Merging Records 10
J. Sharing and Disclosure 11
K. Redress 12
L. Security Safeguards 13
M. Information Retention and Destruction 14
N. Accountability and Enforcement 15
O. Training 16
Appendix A – Terms and Definitions 17
Appendix B – Laws Relevant to Seeking, Retaining, and Disseminating Justice Information 26

A. Purpose Statement

a. The mission of the New Hampshire Information and Analysis Center (NH IAC) is to provide an integrated, all-crimes/all-hazards, information sharing network to collect, analyze and disseminate information derived from multiple sources to stakeholders in a timely manner, in an effort to protect the citizens and the critical infrastructure of New Hampshire, while ensuring the protection of civil rights and civil liberties. *T*his 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 (see definitions of "Fair Information Practice Principles" [(FIPPs)] and "Protected Information" in Appendix A, Terms and Definitions).

The purpose of this P/CRCL protection policy is to promote the NH IAC and user conduct that complies with applicable federal, state, local, tribal, and territorial law (see Appendix B – Laws Relevant to Seeking, Retaining, and Disseminating Justice Information**)** and assists the center and its users in:

i. Increasing public safety and improving national security.

ii. Minimizing the threat and risk of injury to specific individuals.

iii. Minimizing the threat and risk of physical or financial injury to law enforcement and others responsible for public protection, safety, or health.

iv. Minimizing the threat and risk of damage to real or personal property.

v. Protecting individual privacy, civil rights, civil liberties, and other protected interests.

vi. Protecting the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information.

vii. Minimizing reluctance of individuals or groups to use or cooperate with the justice system.

viii. Supporting the role of the justice system in society.

ix. Promoting governmental legitimacy and accountability.

x. Not unduly burdening the ongoing business of the justice system.

xi. Making the most effective use of public resources allocated to public safety agencies.

xii. Evaluating critical infrastructure in the state and assisting the Director of Homeland Security and Emergency Management, law enforcement and the private sector in protecting these assets.

xiii. Minimize the threats associated with special events.

B. Policy Applicability and Legal Compliance

a. The NH IAC's Privacy, Civil Rights and Civil Liberties (P/CRCL) Policy applies to the following NH IAC components:

i. **Personnel**: All personnel assigned to the NH IAC will retain a copy of this policy for their reference. Additionally, all personnel (full or part-time) shall attend annual training in Title 28 US Code part 23 (28 CFR 23) and shall sign a copy of this policy acknowledging their receipt, understanding and agreement to comply with this policy.

ii. **Systems**: All systems managed or operated by the NH IAC. Personnel providing information technology services to the NH IAC and private contractors accessing the system will also comply with this policy. The NH IAC will adhere to this policy when working with or operating on another agency's/organizations system unless the other agency's policies are more stringent with regards to the protection of privacy, civil rights and civil liberties.

iii. **Participating Agencies and Entities**: The participating agencies and entities are those entities and users within the State involved in public safety, homeland security, emergency management, emergency

preparedness, emergency response, critical infrastructure and key resources and public health participants in the NH IAC and the NH IAC Intelligence Liaison Officer Program.

b. The NH IAC and all participating agencies, employees and users will comply with all applicable federal and state law (see Appendix B) protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing and disclosure of information.

c. The NH IAC will provide a printed or electronic copy of this policy to all center and non-center personnel who provide services and to participating agencies and individual users and will require both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and the applicable provisions it contains.

d. The NH IAC has adopted internal operating policies that are in compliance with all applicable laws protecting privacy, civil rights and civil liberties (including but not limited to NH RSA 651-F, NH RSA 260:14, NH RSA 91-A, NH RSA 354-A) in the collection, use, analysis, retention, destruction, sharing and disclosure of information in the system.

e. All NH IAC personnel, participating agency personnel, personnel providing information technology services to the center, private contractors, agencies from which center information originates, and other authorized users will comply with applicable laws protecting privacy, civil rights, and civil liberties, including but not limited to NH RSA 651-F, NH RSA 260:14, NH RSA 91-A, NH RSA 354-A.

C. Governance and Oversight

a. The governance and oversight of the NH IAC is documented within NH RSA 651-F:3 and 651-F:4.

   i. The intelligence subcommittee of the advisory council on emergency preparedness and security (ACEPS) established under RSA 21-P:48 shall serve as an advisory committee to the information and analysis center, meeting periodically at the call of the chair or the commissioner of the department of safety to review the operations of the center and provide advice to the commissioner regarding security, privacy, data technology, the protection of civil rights and civil liberties, and other matters.

   ii. The attorney general or designee, and a representative of a civil liberties organization, appointed by the governor and council, shall meet with the intelligence subcommittee of ACEPS at least annually to receive reports regarding the operation of the center and provide added input to best insure the protection of civil rights, civil liberties and personal privacy.

   iii. The assistant commissioner of the department of safety shall provide ongoing oversight over the operations of the center, and shall ensure that the center compiles a report on its activities to be incorporated with the department of safety's annual report to the governor and council.

b. The management of the NH IAC shall be the joint responsibility of the following three officials: The Director of State Police and the Director of Homeland Security and Emergency Management, in a collaborative effort reporting to the Assistant Commissioner of Safety. The day-to-day operations of the NH IAC shall fall under the management of a State Police officer of the rank of Sergeant or above assigned by the Director of State Police. This individual is identified within this document as the NH IAC director.

c. The NH IAC director exercises direct authority over the employees and persons from other agencies assigned to detached duties at the NH IAC specializing in anti-terrorism, criminal and traffic crash activities and over the employees and persons from other agencies assigned to detached duties at the NH IAC specializing in all-hazards activities. The NH IAC director shall function as the single line authority for issues related to compliance with federal regulations pertaining to the gathering and release of criminal and terrorism intelligence information, adherence to the National Criminal Intelligence Sharing Plan and 28 CFR Part 23.

d. The State Police NH IAC director is trained to serve as the Privacy Officer for the NH IAC and reports to the Colonel of the State Police.

e. The Privacy Officer, along with the NH IAC privacy committee, is responsible for the direct oversight of the P/CRCL policy and will liaise with the community to ensure that privacy, civil rights and civil liberties are protected. The Privacy Officer, in coordination with the privacy committee, is responsible for reviewing and updating the policy, at least annually, as needed to address information collection, retention and dissemination procedures.

f. The Privacy Officer receives reports reporting alleged errors and violations of the provisions of this policy, receives and coordinates complaint resolution under the center's redress policy, and serves as the liaison for the Information Sharing Environment, ensuring that privacy protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy-enhancing technologies.

g. The NH IAC Privacy Officer ensures that enforcement procedures and sanctions outlined in Section N.3 are adequate and enforced.

h. The NH IAC Privacy Officer is identified as:

Name:	Marilynn Burkowski
Address:	110 Smokey Bear Boulevard, Concord, NH
Mailing Address:	33 Hazen Drive Concord, NH 03305
Telephone:	603 223-3859
Email:	Marilynn.l.burkowski@dos.nh.gov

D. Definitions

a. Primary terms and definitions used in this policy are located in Appendix A

E. Information

a. The NH IAC will seek or retain information that:

i. Is based on a possible threat to public safety or the enforcement of the criminal law, or

ii. Is based on a reasonable suspicion, as defined in NH RSA 651-F:5, VIII and this policy, 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 the information is relevant to the criminal (including terrorist) conduct or activity, or

iii. 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

iv. Is useful in crime analysis or in the administration of criminal justice and public safety (including topical searches), and

v. The source of the information is reliable and verifiable or limitations on the quality of the information are identified, and

vi. The information was collected in a fair and lawful manner, with the knowledge and consent of the individual, if appropriate.

b. The NH IAC may receive protected information that is based on a level of suspicion that is less than "reasonable suspicion", as this term is customarily used by law enforcement in making investigatory stops, such as tips and leads or suspicious activity report (SAR) information, subject to policies and procedures specified in this policy. However, the NH IAC may collect and retain tips and leads and SAR information as set forth subsequently herein, as long as it meets the definition of "reasonably suspected" in NH RSA 651-F:1, VIII, and as defined in this policy.

c. The NH IAC will not seek or retain, and information- originating agencies will agree not to submit, information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, or sexual orientation.

   When participating on a federal law enforcement task force or when documenting a 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.

d. The NH IAC applies labels to center-originated information (or ensures that the originating agency has applied labels) to indicate to the accessing authorized user that:

   i. The information is "protected information," to include "personal data" on any individual (as defined in Appendix A) and, to the extent expressly provided in this policy, includes organizational entities.

   ii. The information is subject to local, state or federal laws restricting access, use or disclosure.

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

   i. Whether the information consists of tips and leads data, suspicious activity reports, criminal history, intelligence information, case records, conditions of supervision, case progress, or other information category.

   ii. The nature of the source as it affects veracity (for example, anonymous tip, trained investigator, public record, private sector).

   iii. The reliability of the source (for example, reliable, usually reliable, unreliable, unknown).

   iv. The validity of the content (for example, confirmed, probable, doubtful, cannot be judged).

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

   i. Protect confidential sources and law enforcement undercover techniques and methods.

   ii. Not interfere with or compromise pending criminal investigations.

   iii. Protect an individual's right of privacy or his/her civil rights and civil liberties.

   iv. Provide legally required protections 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.

g. The labels assigned to existing information under Section E(f) above will be reevaluated whenever:

   i. New Information is added that has an impact on access limitations or the sensitivity of disclosure of the information.

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

h. The access labels will be used to control what information a class of users can have access to; and to whom the information can be disclosed and under what circumstances.

i. NH IAC personnel are required to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of tips and leads and suspicious activity report (SAR) information. Center personnel will:

   i. Prior to allowing access to or dissemination of the information, ensure that attempts to validate or refute the information have taken place, that it rises to the level of "reasonably suspected" as defined in NH RSA 651-F:1, VIII and that the information has been assessed for sensitivity and confidence by subjecting it to an evaluation or screening process to determine its credibility and value and categorize the information as unsubstantiated or uncorroborated if attempts to validate or determine the reliability of the information have been unsuccessful. The center will use a standard reporting format and data collection codes for terrorism-related SAR information.

   ii. Store the information using the same storage method used for other intelligence data which rises to the level of "reasonably suspected" as defined in NH RSA 651-F:1, VIII and in this policy, though with restricted access, and which includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information.

   iii. Not allow remote access to or disseminate the information outside of the NH IAC other than to appropriate law enforcement investigators for vetting, to determine if it rises to the level of "reasonably suspected".

   iv. Provide access to or disseminate the information in response to an interagency inquiry for law enforcement, homeland security, or public safety and analytical purposes or provide an assessment of the information to any agency, entity, individual, or the public when credible information indicates potential imminent danger to life or property.

   v. Retain information for up to 90 days in order to work an unvalidated tip, lead, or SAR information to determine its credibility and value, raise it to the level of reasonably suspected as defined in this policy and NH RSA 651-F:1, VIII / develop reasonable suspicion, or assign a "disposition" label (for example, undetermined or unresolved, cleared or unfounded, verified, or under active investigation) so that a subsequently authorized user knows the status and purpose for the retention and will retain the information based on the retention period associated with the disposition label.

   vi. Adhere to and follow the center's physical, administrative, and technical security measures to ensure the protection and security of tips, leads, and SAR information. Non-validated tips, leads, and SAR information will be secured in a system that is the same as or similar to the system that secures data that rises to the level of "reasonably suspected", although its access with be restricted until it reaches that level for a period not to exceed 90 days.

j. The NH IAC incorporates the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious activities and incidents (SAR process) into existing processes and systems used to manage other crime-related information and criminal intelligence, thus leveraging existing policies and protocols utilized to protect the information, as well as information privacy, civil rights, and civil liberties.

k. The NH IAC will identify and review protected information that may be accessed from or disseminated by the center prior to sharing that information through the Information Sharing Environment (ISE) for terrorism related SAR information. Further, the center will provide notice mechanisms, including but not limited to metadata or data field labels, which 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.

l. The NH IAC requires certain basic descriptive information (metadata tags or labels) to be entered and electronically associated with data (or content) for which there are special laws, rules, or policies regarding access, use, and disclosure, including terrorism-related information shared through the ISE. The types of information include:

i. The name of the originating center, department or agency, component, and subcomponent.

ii. The date the information was collected and, where feasible, the date its accuracy was last verified.

iii. The title and contact information for the person to whom questions regarding the information should be directed.

iv. If applicable, the name of the center's justice information system from which the information is disseminated. For terrorism-related specific information, it will be shared through the ISE vie eGuardian. For other criminal information, to include terrorism precursor crimes, it will be shared through the New Hampshire Law Enforcement Information network Exchange (LINX).

m. The NH IAC 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.

n. The NH IAC will gather and disseminate non-criminal data such as traffic crash information, weather information, and other data and information relevant and useful to the non-criminal (all-hazard) deployment of public safety resources; provided however, that the NH IAC shall not receive, obtain, use, retain or disseminate any personally identifiable data in connection with such activities other than that publicly available for individuals licensed by the state to engage in certain occupations and professions that may be needed to respond to emergencies, and contact data regarding persons in charge of or responsible for responding to incidents at critical infrastructure sites.

o. The NH IAC will keep a record of the source of all information sought and collected by the center.

F. Acquiring and Receiving Information

a. The NH IAC serves as the nucleus for the receipt and dissemination of information related to all-hazard, all-crime and terrorism activities in the State. The NH IAC works with various federal, state and local law enforcement agencies, as well as non-law enforcement groups such as the public health department, fire departments, EMS, and the private sector.

b. Information-gathering (acquisition) and access and investigative techniques used by the NH IAC and information-originating agencies will remain in compliance with and will adhere to applicable laws and guidance, including, but not limited to:

i. 28 CFR Part 23 regarding criminal intelligence information

ii. The OECD Fair Information Principles (under certain circumstances, there may be exceptions to the Fair Information Principles, based, for example, on authorities paralleling those provided in the federal Privacy Act; state, local, and tribal law; or center policy).

iii. Criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) *National Criminal Intelligence Sharing Plan* (NCISP).

iv. Constitutional provisions; NH RSA 651-F; and administrative rules, as well as regulations and policies that apply to multijurisdictional intelligence and information databases.

c. The NH IAC Tips , Leads and SAR process provides for human review and vetting to ensure that information is both legally gathered and, where applicable, determined to have a potential terrorism or law enforcement nexus. Law enforcement officers and appropriate center and participating agency staff will be trained to recognize those behaviors and incidents that are indicative of precursor activities related to terrorism or criminal activity.

d. The NH IAC's Terrorism 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. Information-gathering and investigative techniques used by the NH IAC will and those used by originating agencies should be the least intrusive means necessary in the particular circumstances to gather information it is authorized to seek or retain.

f. External agencies that access the NH IAC's information or share information with the center are governed by the laws and rules governing those individual agencies, including applicable federal and state laws.

g. The NH IAC will contract only with commercial database entities that provide an assurance that their methods for gathering personally identifiable information comply with applicable local, state, tribal, territorial, and federal laws, statutes, and regulations and that these methods are not based on misleading information-gathering practices.

h. The NH IAC will not directly or indirectly receive, seek, accept, or retain information from:

    i. An individual who or nongovernmental entity that may or may not receive a fee or benefit for providing the information, except as expressly authorized by law or center policy.

    ii. An individual who or information provider that is legally prohibited from obtaining or disclosing the information.

G. Information Quality Assurance

a. The NH IAC will make every reasonable effort to ensure that information sought or retained is:

    i. derived from dependable and trustworthy sources of information;

    ii. accurate;

    iii. current;

    iv. complete, including the relevant context in which it was sought or received and other related information;

    v. open source information or public information may be used but will be noted as such when the validity is unconfirmed; and,

    vi. merged with other information about the same individual or organization only when the applicable standard in Section I has been met.

b. At the time of retention in the system, the information will be labeled regarding its level of quality (accuracy, completeness, currency, and confidence [verifiability and reliability])

c. The NH IAC investigates, in a timely manner, alleged errors and deficiencies (or refers them to the originating agency) and corrects, deletes, or refrains from using protected information found to be erroneous or deficient.

d. The NH IAC will make every reasonable effort to ensure that only authorized users are allowed to add, change or delete information in the system.

e. The NH IAC will make every reasonable effort to ensure that information will be deleted from the system if the center learns that:

    i. the information is erroneous, misleading, obsolete or otherwise unreliable;

    ii. the source of the information did not have authority to gather the information or to provide the information to the agency; or,

    iii. the source of the information used prohibited means to gather the information.

f. The labeling of retained information will be reevaluated by the NH IAC or the originating agency when new information is gathered that has an impact on confidence (source reliability and content validity) in previously retained information.

g. Originating agencies external to the NH IAC are responsible for reviewing the quality and accuracy of the data provided to the center. The center will review the quality of information it has received from an originating agency

and advise the appropriate contact person in the originating agency, in writing or electronically, if its data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable.

h. The NH IAC 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.

H. Collation and Analysis

a. Information, to include personally identifiable information, sought or received by the NH IAC or from other sources will only be analyzed:

   i. by qualified individuals who have successfully passed a background check and have been properly trained;

   ii. to 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 terrorist, activities generally; and,

   iii. to further crime and terrorism prevention, enforcement, force deployment or prosecution objectives and priorities established by the agency.

b. Information subject to collation and analysis is information as defined and identified in Section E of this policy.

c. Information acquired or received by the NH IAC or accessed from other sources is analyzed according to priorities and needs and will be analyzed only to:

   i. Further crime prevention (including terrorism), law enforcement, public safety, force deployment, or prosecution objectives and priorities established by the center.

   ii. 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 terrorist) activities.

   iii. The NH IAC will gather, analyze and disseminate non-criminal data such as traffic crash information, weather information, and other data and information relevant and useful to the non-criminal (all-hazard) deployment of public safety resources; provided however, that the NH IAC shall not receive, obtain, analyze, use, retain or disseminate any personally identifiable data in connection with such activities other than that publicly available for individuals licensed by the state to engage in certain occupations and professions that may be needed to respond to emergencies, and contact data regarding persons in charge of or responsible for responding to incidents at critical infrastructure sites.

d. The NH IAC requires that all analytical products be reviewed and approved by the Privacy Officer or trained designee to ensure that they provide appropriate privacy, civil rights, and civil liberties protections prior to dissemination or sharing by the center.

I. Merging Records

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

b. The set of identifying information sufficient to allow merging will utilize reasonable steps to identify the subject, and may include the name (full or partial) and, in most cases, one or more of the following: date of birth; law enforcement or corrections system identification number; individual identifiers such as fingerprints, photographs, physical description, height, weight, eye and hair color, race, ethnicity, tattoos, marks or scars; social security number; driver's license number; other biometrics such as DNA, retinal scan, or facial recognition. Identifiers or

characteristics that, when combined, could clearly establish that the information from multiple records is about the same organization may include the organization's name, federal or state tax ID number, office address and telephone number.

c. If the matching requirements are not fully met but there is a strong partial match, the information may be associated by the NH IAC if accompanied by a clear statement that is has not been adequately established that the information relates to the same individual or organization.

J. Sharing and Disclosure

a. Access to or disclosure of records retained by the NH IAC will be provided only to persons within the center or in other governmental agencies who are authorized to have access and only for legitimate law enforcement, public protection, public prosecution, public health, or justice purposes and only for the performance of official duties in accordance with law and procedures applicable to the agency for which the person is working.

    i. 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.

    ii. Agencies external to the NH IAC may not disseminate NH IAC information accessed or disseminated from the NH IAC without prior approval from the originator of the information.

b. Credentialed, role-based access criteria (need to know / right to know) will be used by the NH IAC as appropriate to control:

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

    ii. The information a class of users can add, change, delete or print.

    iii. To whom, individually, the information can be disclosed and under what circumstances.

c. The NH IAC adheres to the current version of the ISE-SAR Functional Standard for its suspicious activity reporting (SAR) process, including the use of a standard reporting format and commonly accepted data collection codes and a sharing process that complies with the ISE-SAR Functional Standard for suspicious activity potentially related to terrorism.

d. Records retained by the NH IAC 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.

    i. 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.

e. Information gathered or collected and records retained by the NH IAC may be accessed or disseminated for specific purposes upon request by persons authorized by law to have such access and only for those uses and purposes specified in the law.

    i. An audit trail sufficient to allow the identification of each individual who requested, accessed, or received information retained by the center.

    ii. The nature of the information requested, accessed, or received; and the specific purpose will be kept for a minimum of 12 months by the center.

f. Information gathered or collected and records retained by the NH IAC may be accessed or disclosed to a member of the public only if the information is defined by law to be a public record or otherwise appropriate for release to further the center's mission and is not exempt from disclosure by law.

    i. Such information may be disclosed only in accordance with the law and procedures applicable to the center for this type of information.

ii. 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.

g. Information gathered or collected and records retained by the NH IAC will not be:

i. Sold, published, exchanged, or disclosed for commercial purposes.

ii. Disclosed or published without prior notice to the originating agency that such information is subject to disclosure or publication, unless disclosure is previously agreed to as part of the normal operations of the agency.

iii. Disseminated to persons not authorized to access or use the information.

h. There are several categories of records that will ordinarily ***not be provided*** to the public:

i. Records required to be kept confidential by law are exempted from disclosure requirements under NH RSA 91-A:5, IV.

ii. Information that meets the definition of "classified information" as that term is defined in the National Security Act, Public Law 235, Section 606, in accord with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal and Private Sector Entities, August 18, 2010, considered confidential by law and would not be disclosed under NH RSA 91-A:5, IV.

iii. Investigatory records of law enforcement agencies that are exempted from disclosure requirements under NH RSA 91-A. However, certain law enforcement records must be made available for inspection and copying under NH RSA 91-A**.**

iv. A record or part of a record the public disclosure of which would have a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack is exempted from disclosure requirements under NH RSA 91-A:5, VI. This includes a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism under NH RSA 91-A:5, VI or an act of agricultural terrorism and, vulnerability assessments, risk planning documents, needs assessments, and threat assessments.

v. Protected federal, state, local, or tribal records, which may include records originated and controlled by another agency that cannot, under NH RSA 91-A:5, IV, be shared without permission.

vi. Records subject to an authorized nondisclosure agreement would be confidential under NH RSA 91-A:5, IV and exempt from disclosure.

i. The NH IAC 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.

K. Redress

a. Disclosure

i. Upon satisfactory verification (driver's license, government issued photo ID or other specified identifying documentation) of his or her identity and subject to the conditions specified in (ii), 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 NH IAC. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information correction. 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.

ii. The existence, content, and source of the information will not be made available by the NH IAC to an individual when:

1. Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution.

2. Disclosure would endanger the health or safety of an individual, organization, or community.

3. The information is in a criminal intelligence information system subject to 28 CFR Part 23 [see 28 CFR § 23.20(e)]
4. The center did not originate and does not have a right to disclose the information.
5. There is another ***authorized*** basis for denial.

iii. If the information does not originate with the center, the requestor will be referred to the originating agency, if appropriate or required, or the center will notify the source agency of the request and its determination that disclosure by the NH IAC or referral of the requestor to the source agency was neither required nor appropriate under applicable law.

b. Corrections

i. If an individual requests correction of information originating with the NH IAC that has been disclosed, the center's Privacy Officer will inform the individual of the procedure for requesting and considering requested corrections, including appeal rights if requests are denied in whole or in part. A record will be kept of all requests for corrections and the resulting action, if any.

c. Appeals

i. The individual who has requested disclosure or to whom information has been disclosed will be given reasons if disclosure or requests for corrections are denied by the NH IAC or the originating agency. The individual will also be informed of the procedure for appeal when the center or originating agency has cited an exemption for the type of information requested or has declined to correct challenged information to the satisfaction of the individual to whom the information relates.

d. Complaints

i. If an individual has a complaint with regard to the accuracy or completeness of terrorism-related protected information that:

1. Is exempt from disclosure,
2. Has been or may be shared through the ISE,
    a. Is held by the NH IAC and
    b. Allegedly has resulted in demonstrable harm to the complainant,

ii. The center will inform the individual of the procedure for submitting and resolving such complaints. Complaints will be received by the center's Privacy Officer at the following address: 33 Hazen Drive, Concord, NH 03305. The Privacy Officer will acknowledge the complaint and state that it will be reviewed but will not confirm the existence or nonexistence of the information to the complainant unless otherwise required by law. If the information did not originate with the center, the Privacy Officer will notify the originating agency in writing or electronically within 10 days and, upon request, assist such agency to correct any identified data/record deficiencies, purge the information, or verify that the record is accurate. All information held by the center that is the subject of a complaint will be reviewed within 30 days and confirmed or corrected/purged if determined to be inaccurate or incomplete, to include incorrectly merged information, or to be out of date. If there is no resolution within 30 days, the center will not share the information until such time as the complaint has been resolved. A record will be kept by the center of all complaints and the resulting action taken in response to the complaint.

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

L. Security Safeguards

a. The NH IAC director is designated and trained to serve as the center's security officer.

b. The NH IAC will operate in a secure facility protected from external intrusion. The center will utilize secure internal and external safeguards against network intrusions.

c. Access to the center's databases from outside the facility will be allowed only over secure networks.

d. The NH IAC will secure unvalidated tips, leads, and SAR information that is being reviewed to determine if it rises to the level of "reasonably suspected" under RSA 651-F for a period not to exceed 90 days in the same repository system using security procedures and policies that are more restrictive than those used for the system that secures intelligence data rising to the level of "reasonably suspected" under NH RSA 651-F and reasonable suspicion under 28 CFR Part 23.

e. The NH IAC shall store information in a manner that ensures it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions.

f. Access to NH IAC information will be granted only to personnel whose:

    i. Positions and job duties require such access;

    ii. Who have successfully completed a background check and appropriate security clearance, if appropriate; and,

    iii. Who have been selected, approved, and trained accordingly.

g. Queries made to the NH IAC's data applications will be logged into the data system identifying the user initiating the query.

h. The NH IAC will utilize logs to maintain audit trails of requested and disseminated information.

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

j. The NH IAC will notify an individual about whom personal information was or is reasonably believed to have been breached or obtained by an unauthorized person and access to which threatens physical, reputational, or financial harm to the person.

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

    ii. To the extent allowable by NH RSA 359-C:20, the NH IAC will immediately notify the originating agency from which the center received personal information of a suspected or confirmed breach of such information.

M. Information Retention and Destruction

a. All applicable information will be reviewed for record retention (validation or purge) by the NH IAC at least every five (5) years, as provided by 28 CFR Part 23 and NH RSA 651-F:5.

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

c. The NH IAC will delete information or return it to the originating agency once its retention period has expired as provided by this policy or as otherwise agreed upon with the originating agency in a participation or membership agreement.

d. No approval will be required from the originating agency before information held by the NH IAC is destroyed or returned in accordance with this policy or as otherwise agreed upon with the originating agency in a participation or membership agreement.

    i. Notification of proposed destruction or return of records may or may not be provided to the originating agency by the NH IAC depending on the relevance of the information and any agreement with the originating agency.

e. A record of information to be reviewed for retention will be maintained by the NH IAC, and for appropriate system(s), notice will be given to the submitter at least 30 days prior to the required review and validation/purge date.

N. Accountability and Enforcement

a. The NH IAC will be open with the public in regard to information and intelligence collection practices. The center's P/CRCL policy will be provided to the public for review on a public Web site and made available, upon request, from the Privacy Officer, contact information below.

Name:	Marilynn Burkowski
Address:	110 Smokey Bear Boulevard, Concord, NH
Mailing Address:	33 Hazen Drive Concord, NH 03305
Telephone:	603 223 3859
Email:	Marilynn.l.burkowski@dos.nh.gov

b. The NH IAC's Privacy Officer or designee will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s) maintained or accessed by the center. The Privacy Officer can be contacted at marilynn.l.burkowski@dos.nh.gov.

c. The audit log of queries made to the NH IAC will identify the user initiating the query.

d. The NH IAC will maintain an audit trail of accessed, requested, or disseminated information. An audit trail will be kept for a minimum of 12 months of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.

e. The NH IAC will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with system requirements and with the provisions of this policy and applicable law. This will include logging access to these systems and periodic auditing of these systems, so as to not establish a pattern of the audits. These audits will be mandated at least semiannually and a record of the audits will be maintained by the Privacy Officer or designee.

f. The NH IAC's personnel or other authorized users shall report errors and suspected or confirmed violations of center policies relating to protected information to the center's Privacy Officer. (see Section C.c)

g. The NH IAC will annually conduct an audit and inspection of the information and intelligence contained in its information system(s). The audit will be conducted at the direction of the Assistant Commissioner of the New Hampshire Department of Safety. The Assistant Commissioner has the option of conducting a random audit, without announcement, at any time and without prior notice to staff of the center. The audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the center's information and intelligence system(s).

h. The NH IAC's privacy committee, guided by the appointed and trained Privacy Officer, will review and update the provisions protecting privacy, civil rights, and civil liberties contained in this policy **annually** and will make appropriate changes in response to changes in applicable law, technology, the purpose and use of the information systems, and public expectations.

i. If center personnel, a participating agency, or an authorized user is found to be in noncompliance with the provisions of this policy regarding the gathering, collection, use, retention, destruction, sharing, classification, or disclosure of information, the NH IAC director will:

    i. Suspend or discontinue access to information by the center personnel, the participating agency, or the authorized user.

ii. Suspend, demote, transfer, or terminate center personnel, as permitted by applicable personnel policies.

iii. Apply administrative actions or sanctions as provided by NH IAC rules and regulations, NH Department of Personnel rules and regulations or as provided in agency/ center personnel policies.

iv. If the authorized user is from an agency external to the NH IAC, request that the relevant agency, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions.

v. Refer the matter to the New Hampshire State Police Investigative Services Bureau Commander and appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

j. The NH IAC 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.

O. Training

a. The NH IAC requires the following individuals to participate in training programs regarding the implementation of and adherence to the P/CRCL policy:

i. All assigned NH IAC personnel;

ii. Personnel providing information technology services to the NH IAC;

iii. Staff in other public agencies or private contractors providing services to the NH IAC; and

iv. Users who are not employed by the NH IAC or a contractor.

b. The NH IAC will provide special training regarding the center's requirements and policies for collection, use, and disclosure of protected information to personnel authorized to share protected information through the Information Sharing Environment.

c. The NH IAC's P/CRCL policy training program will cover:

i. Title 28 U.S. Code (CFR 28, Part 23).

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

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

iv. Originating and participating agency responsibilities and obligations under applicable law and policy.

v. How to implement the policy in the day-to-day work of the user whether a paper or systems user.

vi. The impact of improper activities associated with infractions.

vii. Mechanisms for reporting violations of center privacy protection policies and procedures.

viii. The nature and possible penalties for policy violations, including possible transfer, termination, and criminal liability.

ix. Updates to the P/CRCL policy, if any, in response to changes in law and implementation experience.

x. ISE Core Awareness Training, available at ise.gov

xi. Subject to course availability, the NH IAC Privacy Officer will also take courses offered by the U.S. Department of Homeland Security addressing:

1. P/CRCL training of trainers
2. Derivative classification marking

d. A record of the training completion will be maintained by the NH IAC Privacy Officer.

Appendix A – Terms and Definitions

Access—Data access is being able to get to (usually having permission to use) particular data on a computer. Web access means having a connection to the World Wide Web through an access provider or an online service provider. Data access is usually specified as read-only and read/write access. With regard to the ISE, access refers to the business rules, means, and processes by and through which ISE participants obtain terrorism-related information, to include homeland security information, terrorism information, and law enforcement information acquired in the first instance by another ISE participant.

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.

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

Agency—The NH IAC and all agencies that access, contribute, and share information in the NH IAC's justice information system.

Audit Trail—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. [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]

Authentication—The process of validating the credentials of a person, computer process, or device. Authentication requires that the person, process, or device making the request provide a credential that proves it is what or who it says it is. Common forms of credentials are digital certificates, digital signatures, smart cards, biometrics data, and a combination of user names and passwords.

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

Center—Refers to the NH IAC and all participating state agencies of the NH IAC.

Civil Liberties—Fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights—the first ten Amendments to the Constitution of the United States. Civil liberties offer

protection to individuals from improper government action and arbitrary governmental interference. Generally, the term "civil rights" involves positive (or affirmative) government action, while the term "civil liberties" involves restrictions on government.

Civil Rights—The term "civil rights" is used to imply that the state has a role in ensuring that all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of race, religion, gender, or other characteristics unrelated to the worth of the individual. Civil rights are, therefore, obligations imposed on government to promote equality. More specifically, they are the rights to personal liberty guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments and by acts of Congress.

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

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

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

Criminal Intelligence Information—Information and data that have been determined through evaluation to be relevant to the identification of actual and impending criminal activity by an individual or group that is reasonably suspected of involvement in criminal or terrorist activity, and meets valid criminal intelligence suspicion criteria. Criminal activity shall not include motor vehicle-related offenses (NH RSA 651-F:1, I). Criminal intelligence records are maintained in a criminal intelligence system per 28 CFR Part 23.

Criminal Intelligence System—The arrangements, equipment, facilities, and procedures used for the receipt, analysis, storage, interagency sharing, or dissemination of criminal intelligence information (NH RSA 651-F:1, II).

Data—Inert symbols, signs, descriptions, or measures; elements of information.

Data Breach—The unintentional release of secure information to an untrusted environment. 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 World Wide Web or on a computer otherwise accessible from the Internet without proper information security precautions; 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; or transfer of such information to the information systems of a possibly hostile agency or environment where it may be exposed to more intensive decryption techniques.

Data Protection—Encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, use, protection, and disclosure of information.

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

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

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

Fair Information Practice Principles—The Fair Information Practice Principles (FIPPs) are contained within the Organisation for Economic Co-operation and Development's (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. These were developed around commercial transactions and the transborder exchange of information; however, they do provide a straightforward description of underlying privacy and information exchange principles and provide a simple framework for the legal analysis that needs to be done with regard to privacy in integrated justice systems. Some of the individual principles may not apply in all instances of an integrated justice system.

The eight FIPPs are:

1. Collection Limitation Principle
2. Data Quality Principle
3. Purpose Specification Principle
4. Use Limitation Principle
5. Security Safeguards Principle
6. Openness Principle
7. Individual Participation Principle
8. Accountability Principle

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

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

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

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

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

Information and Analysis Center (IAC)— An organizational entity within the department of safety that compiles, analyzes, and disseminates information in support of efforts to anticipate, identify, prevent, mitigate, respond to, and recover from natural and human-caused threats to the state and its people or to the United States, on behalf of the single government agency and also operates an inter-jurisdictional intelligence sharing system on behalf of 2 or more participating agencies, whether called a criminal intelligence system, information and analysis center, fusion center, or by any other name (NH RSA 651-F:1, III).

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

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

Intelligence Data—Information and data gathered from a number of sources that, when analyzed and evaluated, provides the basis for decision making to help ensure the safety and well-being of the people of New Hampshire from actual or impending criminal or terrorist activity. (NH RSA 651-F:1, IV)

Intelligence-Led Policing (ILP)—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.

Inter-jurisdictional Intelligence System— An intelligence system that involves 2 or more participating agencies representing different governmental units or jurisdictions. (NH RSA 651-F:1, V)

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

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

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

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

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

Least Privilege Administration—A recommended security practice in which every user is provided with only the minimum privileges needed to accomplish the tasks he or she is authorized to perform.

Logs—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—Applies to all forms of information storage. This includes electronic systems (for example, databases) and nonelectronic 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.

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

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

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

Participating Agency—An agency of a local, county, state, federal, or other governmental unit that exercises homeland security, emergency management, law enforcement, or criminal investigation authority and is authorized to submit and receive criminal intelligence data through an inter-jurisdictional intelligence system. A participating agency may be a member or non-member of an inter-jurisdictional intelligence system. (NH RSA 651-F:1, VI)

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

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

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

Personally Identifiable Information—Data or information that contains a person's name, date or place of birth, social security number, address, employment history, credit history, financial information, account numbers, cellular telephone, voice over Internet protocol or landline telephone numbers, biometric identifiers including fingerprints, facial photographs or images, retinal scans, DNA/RNA, or other identifying data unique to that individual (NH RSA 651-F:1, VII). One or more pieces of

information that, when considered together or in the context of how the information is presented or gathered, are sufficient to specify a unique individual. The pieces of information can be:

- Personal characteristics (such as height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation, place of birth, mother's maiden name, distinguishing features, and biometrics information, such as fingerprints, DNA, and retinal scans).
- A unique set of numbers or characters assigned to a specific individual (including name, address, phone number, social security number, e-mail address, driver's license number, financial account or credit card number and associated PIN number, Integrated Automated Fingerprint Identification System [AFIS] identifier, or booking or detention system number).
- Descriptions of event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records).
- Descriptions of location(s) or place(s) (including geographic information systems [GIS] locations, electronic bracelet monitoring information, etc.)

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

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

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

Privacy Protection—A process of maximizing the protection of privacy, civil rights, and civil liberties when collecting and sharing information in the process of protecting public safety and public health.

Protected Information—Protected information includes Personal Data about individuals that is subject to information privacy or other legal protections by law, including the U.S. Constitution and the New Hampshire Constitution; applicable federal statutes and regulations, such as civil rights laws, 28 CFR Part 23; and applicable state and local laws and ordinances. Protections may also be extended to organizations by center policy or state and local law.

Public—Public includes:

- Any person 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:

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

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

Reasonably Suspected— Information received and evaluated by a law enforcement officer or intelligence analyst in consideration of his or her training and experience and the facts and circumstances under which it was received that would cause a prudent person to conclude that there are sufficient facts to believe that the information is relevant to and will aid in the detection, discovery, or interruption of actual, planned, or impending criminal or terrorist activity by an individual or group. (NH RSA 651-F:1, VIII)

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

Redress—Laws, policies, and procedures that address public agency responsibilities with regard to access/disclosure and correction of information and the handling of complaints from persons regarding protected information about them which is under the center's control and which is exempt from disclosure and not disclosed to the individual to whom the information pertains.

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

Retention—Refer to Storage.

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

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

Role-Based Access—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—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—Source agency refers to the agency or organizational entity that originates intelligence, tips, leads and SAR (and when authorized, ISE-SAR) information.

Storage—In a computer, storage is the place where data is held in an electromagnetic or optical form for access by a computer processor. There are two general usages:

- Storage is frequently used to mean the devices and data connected to the computer through input/output operations—that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-computer storage. This is probably the most common meaning in the IT industry.
- In a more formal usage, storage has been divided into (1) primary storage, which holds data in memory (sometimes called random access memory, or RAM) and other "built-in" devices such as the processor's L1 cache, and (2) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations.
- Primary storage is much faster to access than secondary storage because of the proximity of the storage to the processor or because of the nature of the storage devices. On the other hand, secondary storage can hold much more data than primary storage.
- With regard to the ISE, storage (or retention) refers to the storage and safeguarding of terrorism-related information—including 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.

Suspicious Activity—Defined in the ISE-SAR Functional Standard (Version 1.5) as "observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity." Examples of suspicious activity include surveillance, photography of sensitive infrastructure facilities, site breach or physical intrusion, cyber attacks, testing of security, etc.

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

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

Terrorism-Related Information—In accordance with 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.

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

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.

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.

Validation of Information— The procedures governing the periodic review of criminal intelligence and personally identifiable data to assure its continuing compliance with system submission criteria. (NH RSA 651-F:1, IX)

Appendix B – Laws Relevant to Seeking, Retaining, and Disseminating Justice Information

Federal

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

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, Memorandum M-01-05, "Guidance on Interagency Sharing of Personal Data–Protecting Personal Privacy," December 20, 2000

Confidentiality of Identifiable Research and Statistical Information, 28 CFR Part 22, Code of Federal Regulations, Title 28, Chapter I, Part 22

C**rime Identification Technology**, 42 U.S.C. § 14601, United States Code, Title 42, Chapter 140, Subchapter I, § 14601

Criminal History Records Exchanged for Noncriminal Justice Purposes, 42 U.S.C. § 14611, United States Code, Title 42, Chapter 140, Subchapter II, § 14611

Criminal Intelligence Systems Operating Policies, 28 CFR Part 23, Code of Federal Regulations, Title 28, Chapter 1, Part 23

Criminal Justice Information Systems, 28 CFR Part 20, Code of Federal Regulations, Title 28, Chapter 1, Part 20

Disposal of Consumer Report Information and Records, 16 CFR Part 682, Code of Federal Regulations, Title 16, Chapter I, Part 682

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

Fair Credit Reporting Act, 15 U.S.C. § 1681, United States Code, Title 15, Chapter 41, Subchapter III, § 1681

Federal Civil Rights laws, 42 U.S.C. § 1983, United States Code, Title 42, Chapter 21, Subchapter I, § 1983

Federal Records Act, 44 U.S.C. § 3301, United States Code, Title 44, Chapter 33, § 3301

Freedom of Information Act (FOIA), 5 U.S.C. § 552, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552

HIPAA, Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 201, United States Code, Title 42, Chapter 6A, Subchapter I, § 201; Public Law 104-191

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

Indian Civil Rights Act of 1968, 25 U.S.C. § 1301, United States Code, Title 25, Chapter 15, Subchapter I, § 1301

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

National Child Protection Act of 1993, Public Law 103-209 (December 20, 1993), 107 Stat. 2490

National Crime Prevention and Privacy Compact, 42 U.S.C. § 14616, United States Code, Title 42, Chapter 140, Subchapter II, § 14616

Privacy Act of 1974, 5 U.S.C. § 552a, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a

Privacy of Consumer Financial Information, 16 CFR Part 313, Code of Federal Regulations, Title 16, Chapter I, Part 313

Protection of Human Subjects, 28 CFR Part 46, Code of Federal Regulations, Title 28, Chapter 1, Volume 2, Part 46

Safeguarding Customer Information, 16 CFR Part 314, Code of Federal Regulations, Title 16, Chapter I, Part 314

Sarbanes-Oxley Act of 2002, 15 U.S.C., Chapter 98, § 7201, United States Code, Title 15, Chapter 98, § 7201

U.S. Constitution, First, Fourth, and Sixth Amendments

USA PATRIOT Act, Public Law 107-56 (October 26, 2001), 115 Stat. 272

State

This comprehensive list may not contain a reference for every New Hampshire Statute, Supreme Court decision, or court rule which makes information confidential or non-public. Questions regarding specific information which is not addressed by these statutes should be referred to legal counsel. This list is based on the New Hampshire Revised Statutes Annotated as amended through the 2009 session of the Legislature. Before relying on this information, verify the authority, check to ensure there have been no subsequent revisions made to the statutes, and check for new court decisions.

7:41 Findings and Purpose

7:47 Disclosure of Records Prohibited; Exceptions

9:4 - Requests for Appropriations and Statement of Objectives and 9:5- Estimates of Income

14:31-a – Audit work papers and notes

21-G:31 - Complaints; Procedure

21-M:8-c Victim of Alleged Sexual Offense

21-M:8-k Rights of Crime Victims

21-M:9 Consumer Protection and Antitrust Bureau

21-I:52-a – Employee Assistance Program; Confidential Communications

21-M:16 Incapacitated Adult

21-J:14 Confidentiality of Department Records for the Department of Revenue

33-A:3-a Disposition and Retention Schedule

72:34 (II) Investigation of Application and Decision by Town Officials

76:16-III (h) By Selectmen or Assessors

77-B:26 Commuter's Income Tax Confidentiality of Department of Revenue Administration Records

82-A:16-a Confidentiality of Records-from 82-A Communications Services Tax

84-A:10 & 84-C:10 Confidentiality of Records under Title V: Taxation

91-A:5 (I)Grand and Petit Jury Records

91-A:5 (II) Parole and Pardon Board Records

91-A:5 (III) Sealed Minutes

91-A:5 (III) Personal School Records of Pupils

91-A:5 (IV) Records pertaining to internal personnel practices; confidential, commercial, or financial information

91-A:5 (IV) Records pertaining to confidential, commercial, or financial information

91-A:5 (IV) Records pertaining to personnel, medical, welfare, library user, videotape sale or rental and other files whose disclosure would constitute invasion of privacy

91-A:5 (V) Teacher Certification Records

91-A:5 (VI) Records pertaining to matters relating to the preparation for and the carrying out of all emergency functions

91-A:5 (VII) Unique pupil identification information

91-A:5 (VIII) Any notes or other materials made for personal use that do not have an official purpose

91-A:5 (IX) Preliminary drafts, notes, and memoranda and other documents not in their final form

98-E:3 Confidential Records under Title VI. Public Officers and Employees

105:13-b Confidentiality of Personnel Files under Title VII. Sheriffs, Constables, and Police Officers

106-F:6 Application for License; Confidential under Title VII. Sheriffs, Constables, and Police Officers

106-H:12 Confidentiality – Enhanced 911 systems

106-K:6 Confidentiality – Enhanced 911 systems

126-J:4 Technical Assistance under Title X Public Health

126:24-d Disclosure of Information From Vital Records

126-A:4 (III), (IV – b)– Dept. of Health and Human Services

126-H:8 Healthy Kids Corporation – Confidentiality

135-C:19-a (II) and (III)NH Mental Health Services System – Disclosure of Certain Information

135-C:63-a (II)- NH Mental Health Services System Proceedings of Quality Assurance Program; Confidentiality

135-C:66 Access of Records under Title X: Public Health

135-E:3 (VI) Involuntary Civil Commitment of Sexually Violent Predators - Notice to County Attorney or Attorney General; Multidisciplinary Teams Established

135-E:15 Involuntary Civil Commitment of Sexually Violent Predators - Release of Records

137-J:9 Confidentiality and Access to Protected Health Information

137-K:7 Brain and Spinal Cord Injuries - Disclosure; Confidentiality

141-B:9 Chronic Disease Prevention, Assessment and Control - Disclosure; Confidentiality

146-C:5 Records Required; Inspections under Title X Public Health

141-C:10 Communicable Diseases – Disclosure

141-F:8 (I, II, V) Human Immunodeficiency Virus Education, Prevention, and Control -Confidentiality; Release of Information

147-C:4 Duties of the Committee under Title X: Public Health

151:2-d Criminal Record Check Required under Title:XI Hospitals and Sanitaria

151:5-c Proceedings of Residential Care Facility Quality Assurance Program; confidentiality under Title XI: Hospitals and Sanitaria

151-D:2 Proceedings of Quality Assurance Program; confidentiality under Title XI: Hospitals and Sanitaria

151-G:5 Confidentiality under Title XI: Hospitals and Sanitaria

151-G:6 Administration under Title XI: Hospitals and Sanitaria

155:74 Complaints; Investigations; Confidentiality

159:6-a confidentiality of Licenses

159-D:2 Confidentiality

161-C:3-a Confidentiality of Records and Information; Information From Financial Institutions under Title XII Public Safety and Welfare

161-F:14 Access to Facilities, Residents, and Records under Title XII Public Safety and Welfare

161-F:57 Access to Files; Confidentiality

161-I:6-a Criminal Record Check Required

167:30 Confidential Character of Public Assistance Record under Title XII: Public Safety and Welfare

169-B:19 Dispositional Hearing under Title XII Public Safety and Welfare

169-C:25 Confidentiality under Title XII: Public Safety and Welfare

169-C:34-a Multidisciplinary Child Protection Teams and Title XII: Public Safety and Welfare

170-B:23 Confidentiality of Records under Title XII: Public Safety and Welfare

170-C:14 Confidentiality of Records under Title XII: Public Safety and Welfare

170-E:7 State Registry and Criminal Records Check; Revocation of Registration and Withholding of State Funds under Title XII: Public Safety and Welfare

170-E:23 Confidentiality and Investigations under Title XII: Public Safety and Welfare

170-E:29 State Registry and Criminal Records Check

170-E:49 Confidentiality and Investigations under Title XII: Public Safety and Welfare

170-G:8-a Record Content; Confidentiality; Rulemaking under Title XII: Public Safety and Welfare

172:8-a Confidentiality of Client Records under Title XII: Public Safety and Welfare

173-B:22 Confidentiality under Title XII Public Safety and Welfare

173-C:2 Privilege under Title XII: Public Safety and Welfare

189:13-a School Employee and Volunteer Background Investigations under Title XV: Education

193-D:7 Confidentiality under Title XV: Education

201-D:11 Library User Records; Confidentiality under Title XVI: Libraries

227-C:11 Confidentiality of Archeological Site Location Information under Title XIX: Public Recreation

236:31 Evasion of Tolls and Charges under Title XX: Transportation

237:16-e Confidentiality of Records under Title XX: Transportation

260:14 – Motor Vehicles under Chapter XXI: Motor Vehicles

263:56-b Revocation or Denial for Drugs or Alcohol Involvement under Title XXI: Motor Vehicles

275:62 Right to Leave Work under Title XXIII: Labor

277-B:15-a Client List; Confidentiality under Title XXIII: Labor

281-A:21-b Confidentiality of Workers' Compensation Claims under Title XXIII: Labor

282-A:117-123 and 91-A:6 Records exempt from inspection

282-A:118 Reports or Statement; Confidentiality under Chapter XXIII: Labor

282-A:119 Summary, Duplication, etc.; Admissibility under Chapter XXIII: Labor

282-A:120 Destruction of Records under Chapter XXIII: Labor

282-A:121 Penalty under Chapter XXIII Labor

282-A:123 Records Unavailable for Legal Process under Chapter XXIII: Labor

282-A:118 Reports or Statement; Confidentiality under Title XXIII: Labor

311 Unauthorized practice of law – investigations confidential

318:5-a Rulemaking Authority under Title XXX: Occupations and Professions

326-B:15 Criminal History Record Checks under Title XXX Occupations and Professions

326-E:5 Duties and Powers of the Board under Title XXX: Occupations and Professions

326-E:7 Rights of Consumers under Title XXX: Occupations and Professions

328-A:15 Rights of Consumers; Confidentiality under Title XXX: Occupations and Professions

328-C:5-a Confidentiality of Information under Title XXX: Occupations and Professions

328-D:3-a Criminal History Record Checks under Title XXX: Occupations and Professions

328-F:24 Investigations and Disciplinary Proceedings under Title XXX: Occupations and Professions

329:13-b Physician Effectiveness Program under Title XXX: Occupations and Professions

329:20-a Report to Blind Services Program, Bureau of Vocational Rehabilitation under Title XXX: Occupations and Professions

329:26 Confidential Communications under Title XXX: Occupations and Professions

329:29 Proceedings of Medical Review Committee under Title XXX: Occupations and Professions

329:29-a Proceedings of Physician Practice Quality Assurance Program; Confidentiality under Title XXX: Occupations and Professions

330-A:32 Privileged Communications under Title XXX: Occupations and Professions

332-B:14 Disciplinary Action; Civil Penalty under Title XXX: Occupations and Professions

332-I:2 Patient Information under Title XXX: Occupations and Professions

339-D:3 Inventory Reporting under Title XXXI: Trade and Commerce

351-A:1 Videotape Rental or Sales Records; Confidentiality under Title XXXI: Trade and Commerce

354-B:2 Civil Action by Attorney General under Title XXXI: Trade and Commerce

356:10 – Official Investigation under Chapter XXXI: Trade and Commerce

358-A:8- Subpoena; Production of Books, Examination of Persons, etc. under Chapter XXXI: Trade and Commerce

361-A:6-a Examinations under Title XXXIII-A: Retail Installment Sales

365:8 Rulemaking Authority under Title XXXIV. Public Utilities

378:43 Information Not Subject to Right-to- Know Law under Title XXXIV. Public Utilities

383:7 Compensation; Assistants under Title XXXV. Banks and Banking; Loan Associations; Credit Unions

383:10-b Confidential Information under Title XXXV. Banks and Banking; Loan Associations; Credit Unions

383:10-e Confidential of Consumer Complaints under Title XXXV. Banks and Banking; Loan Associations; Credit Unions

384:60-a Examination of Out-of-State Banks and Bank Holding Companies under Title XXXV. Banks and Banking; Loan Associations; Credit Unions

384-F:33 Confidentiality of Examination Reports under Title XXXV. Banks and Banking; Loan Associations; Credit Unions

392:9-a Confidentiality under Title XXXV. Banks and Banking; Loan Associations; Credit Unions

397-A:5 License Application; Requirements; Investigation under Title XXXV. Banks and Banking; Loan Associations; Credit Unions

397-A:20 Administration by Commissioner; Rulemaking under Title XXXV. Banks and Banking; Loan Associations; Credit Unions

399-A:3 Application and Fees under Title XXXVI. Pawnbrokers and Moneylenders

399-D:5 License Application; Requirements; Investigation under Title XXXVI. Pawnbrokers and Moneylenders

400-A:15-b Confidentiality of Provider's Personal Information under Title XXXVII. Insurance

400-A:25 – Certain Records of the Insurance Dept. under Chapter XXXVII: Insurance

400-A:36-c Confidentiality under Title XXXVII. Insurance

400-A:37 Examinations under Title XXXVII. Insurance

401-B:7 Confidential Treatment under Title XXXVII. Insurance

402-C:14 Conduct of Hearings in Summary Proceedings under Title XXXVII. Insurance

402-D:16 Record Retention under Title XXXVII. Insurance

404-F:8 Confidentiality; Prohibition on Announcements; Prohibition on Use in Ratemaking under Title XXXVII. Insurance

408-C:8 Commission Records and Enforcement under Title XXXVII. Insurance

420-J:5-e General Provisions Regarding External Review under Title XXXVII. Insurance

420-J:10 Confidentiality of Insurer Records under Title XXXVII. Insurance

420-J:11 Confidentiality of Insurance Department Records under Title XXXVII. Insurance

436:123 Confidentiality under Title XL. Agriculture, Horticulture and Animal Husbandry

485-A:18 Investigation and Inspection; Records under Title L. Water Management and Protection

490-C:5-b Confidentiality and Disclosure of Information under Title LI. Courts

463:9 Confidentiality of Proceedings under Title XLIV. Guardians and Conservators

516:36 - Written Policy Directives to Police Officers and Investigators

519-B:8 Confidentiality and Admissibility under Title LIII. Proceedings in Court

522:1 Authority for Test under Title LIII. Proceedings in Court

651-C:2 DNA Analysis Required under Title LXII. Criminal Code

651-F Information and Analysis Center

RULE 40. PROCEDURAL RULES OF COMMITTEE ON JUDICIAL CONDUCT under Rules of the Supreme Court of the State of New Hampshire

RULE 8-2. CONFIDENTIALITY OF REPORTS

Family Division Rule 5.8 CONFIDENTIALITY under New Hampshire Court Rules

PROTOCOL 5. CONFIDENTIALITY under New Hampshire Court Rules

GUIDELINE II. RECORDS SUBJECT TO INSPECTION under New Hampshire Court Rules

Union Leader Corp. v.Fenniman, 136 N.H. at 626, 620 A.2d at 1041

Pivero v. Largy, 143 N.H. 187, 191 (1998)

Hounsell v. North Conway Water Precinct, 154 N.H. 1, 4 (2006)

Goode v. LBA, 148 N.H. 551, (2002)

Chambers v. Gregg (1992) 135 N.H. 478, 606 A.2d 811

Lodge v. Knowlton, 118 N.H. 544 (1978)

Murray v, State Police, 154 N.H. 579, 582 (2006)