NEW YORK STATE INTELLIGENCE CENTER

INFORMATION and INTELLIGENCE

PRIVACY POLICY

NEW YORK STATE INTELLIGENCE CENTER
INFORMATION and INTELLIGENCE PRIVACY POLICY

Table of Contents

NEW YORK STATE INTELLIGENCE CENTER
INFORMATION and INTELLIGENCE PRIVACY POLICY

A. Purpose

The purpose of the New York State Intelligence Center (NYSIC) is to collect, evaluate, analyze, and disseminate information and intelligence data regarding criminal and terrorist activity relevant to New York State while following the *Fair Information Practices* to ensure the rights and privacy of citizens are protected.

The purpose of the privacy, civil rights, and civil liberties policy is to promote the NYSIC, agency and user conduct that complies with federal, state, local and tribal laws and assists the NYSIC and its users in:

- Ensuring the privacy, civil rights, civil liberties, and other protected interests of individuals and organizations;
- Increasing public safety and improving national security;
- Protecting the integrity of systems for the observation and reporting of terrorism-related criminal activity and information;
- Encouraging individuals or community groups to trust and cooperate with the justice system;
- Protecting the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information;
- Promoting governmental legitimacy and accountability; and
- Making the most effective use of public resources allocated to public safety agencies.

B*. Policy Applicability and Legal Compliance*

1**.** All NYSIC personnel, participating agency personnel, personnel providing information technology services to the NYSIC, private contractors, and other users authorized by the Director of the NYSIC and the NYSIC Security Officer (hereafter "NYSIC authorized users") will comply with NYSIC's privacy policy concerning information the NYSIC collects, receives, maintains, archives, accesses, or discloses to NYSIC authorized users, governmental agencies (including Information Sharing Environment [ISE] participating agencies), and participating justice and public safety agencies; or to private contractors and the general public.

2. The NYSIC will provide a printed copy of this policy to all NYSIC authorized users and participating agencies and will require both a written acknowledgement of receipt of this policy and a signed agreement to comply with this policy (see Appendix D).

3. All NYSIC personnel, authorized users, agencies that originate information and other users are to comply with applicable laws protecting the privacy, civil rights, and civil liberties of individuals and organizations (see Appendix B). This includes, but is not limited to:

- US CONST. and US CONST. Amend. I-XXVII
- The Privacy Act of 1974 (5 USC 552a)
- US Executive Order 12958 "Classified National Security Information"

- USDOJ Criminal Intelligence Systems Operating Policies, 28 CFR Part 23 (1998)
- NY State Penal Law, Part III, Title J - Article 156
- NY Public Officer's Law, Articles 6 and 6-A

4. The NYSIC's internal operating policies are to comply with applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to, New York State and Federal privacy, civil rights, and civil liberties laws, statutes and regulations (see Appendix B).

C*. Governance and Oversight*

1. Primary responsibility for the operation of the NYSIC, its justice systems, operations, and coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, sharing, or disclosure of information; the periodic review and purging of information; the information-sharing environment (ISE); and the enforcement of this policy is assigned to the Director of the New York State Intelligence Center, who is an employee of the New York State Police.

2. The NYSIC has designated a Privacy Officer and a Security Officer appointed by the Director of the NYSIC. The Privacy and Security Officers receive and investigate allegations regarding violations of this policy, and report findings to the Director of the NYSIC. The NYSIC Privacy and Security Officers can be reached by contacting the NYSIC at 518-786-2100, or via mail: Attn. [Privacy / Security] Officer, 630 Columbia Street Ext., Latham, NY, 12110. A yearly Privacy Policy review will be conducted by these officers, and any necessary updates will be made.

3. The Privacy and Security Officers are the liaisons to citizen and community privacy advocacy groups to ensure that privacy and civil rights are protected within the provision of this policy and within the NYSIC's information collection, retention, and dissemination processes and procedures.

4. The Privacy and Security Officers receive specific training in privacy and security policies and procedures and adhere to enforcement procedures outlined in Section N-3, Enforcement (page 14). The Privacy and Security Officers shall serve as the liaisons for the ISE, coordinating their efforts to ensure that privacy and security protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy and security enhancing technologies.

D*. Definitions*

1. Key terms and definitions used in this policy document can be found in Appendix A (page 16).
2. For purposes of this privacy policy, the crime of terrorism shall be defined by NYS Penal Law, §490.25 and terrorism information and terrorism-related information shall be defined in Appendix A of this policy.

E*. Information*

1. The NYSIC will only retain information that is:

- Based on a criminal predicate or possible threat to public safety; or

- Based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and the information is relevant to the criminal or terrorist conduct or activity; or
- Relevant to the investigation and prosecution of suspected criminal or terrorist incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime; or
- Deemed to be reliable and verifiable or limitations on the quality of the information are identified; and
- Collected in a fair and lawful manner, and, if appropriate, with the knowledge and consent of the individual.

The NYSIC may retain information that is based on a level of suspicion that is less than "reasonable suspicion," such as tips and leads or suspicious activity report (SAR) information subject to the policies and procedures specified in Section E-7 (page 6).

2. The New York State Police have a long standing policy against racial profiling and discrimination. In no instance will the NYSIC seek or retain information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenships, places of origin, ages, disabilities, genders, or sexual orientations.

3. The NYSIC labels agency-originated information (or ensures that the originating agency has applied labels) indicating to the accessing authorized user that the information is protected (as defined by the ISE Privacy Guidelines) and is subject to laws restricting access, use, or disclosure.

4. NYSIC personnel, upon receipt of information, will access the information to review its nature, usability, and quality. Personnel will assign categories to the information (or ensure that the originating agency will assign categories to the information) to reflect the assessment, such as:

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

5. At the time a decision is made to retain information, it will be labeled (by record, dataset, or record keeping system), to the maximum extent feasible, pursuant to applicable limitations on access and sensitivity of disclosure to:

- Protect confidential sources and police undercover techniques and methods;
- Not interfere with or compromise pending criminal investigations;
- Protect an individual's right of privacy, civil rights, and civil liberties; and
- Provide legally required protection based on the individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.

6. The classification of existing information will be reevaluated whenever:

- New information is added that has an impact on access limitations or the sensitivity of disclosure of the information; or
- There is a change in the use of the information affecting access or disclosure limitations; for example, the information becomes part of court proceedings.

7. NYSIC personnel are required to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of tips, leads, potential intelligence, and suspicious activity report (SAR) information.

- Prior to allowing access to or dissemination of the information, ensure that attempts to validate or refute the information have taken place and that the information has been assessed for sensitivity and confidence by subjecting it to an evaluation or screening process to determine its credibility and value. The information shall be categorized as unsubstantiated or uncorroborated if attempts to validate or determine the reliability of the information have been unsuccessful. The NYSIC will use a standard reporting format and data collection codes for SAR information.
- Open source information will be vetted in the same manner as all intelligence information received or obtained by the NYSIC.
- Store the information using the same storage method used for data that rises to the level of reasonable suspicion and includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information.
- Allow access to or disseminate the information using the same (or a more restrictive) access or dissemination standard that is used for data that rises to the level of reasonable suspicion (for example, “need-to-know” and “right-to-know” access or dissemination).
- Regularly provide access to or disseminate the information in response to an interagency inquiry for law enforcement, homeland security, or public safety and analytical purposes or provide an assessment of the information to any agency, entity, individual, or the public when credible information indicates potential imminent danger to life or property.
- Retain information long enough to work a tip, lead, potential intelligence, or SAR information to determine its credibility and value, assign a “disposition” label (for example, undetermined or unresolved, cleared or unfounded, or under active investigation) so that a subsequently authorized user knows that status and purpose for the retention and will retain the information based on the retention period associated with the disposition label.
- Adhere to and follow the NYSIC’s physical, administrative, and technical security measures that are in place for the protection and security of tips and leads information. Tips, leads, potential intelligence, and SAR information will be secured in a system that is the same or similar to the system that secures data that rises to the level of reasonable suspicion.

Specific details regarding the Suspicious Activity Reporting of tips and leads can be found in the *New York State Intelligence Center (NYSIC) ISE-SAR Privacy, Civil Rights, and Civil Liberties Protection Policy* (see Appendix C).

8. The NYSIC 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. Details regarding specific protection of constitutional rights, including personal privacy, civil rights, and civil liberties, can be found in the *NYSIC ISE-SAR Privacy Policy.*

9. The NYSIC will identify and review protected information that is originated by the NYSIC prior to sharing that information through the Information Sharing Environment. Further, the NYSIC will provide notice sensitivity

markings that will enable ISE authorized users to determine the sensitivity of the protected information and how to handle the information in accordance with applicable legal requirements.

10. The NYSIC requires certain details to be entered and electronically associated with information and intelligence data. The types of information should include:

- The name of the originating agency and subunit(s), if appropriate.
- The name of the agency's justice information system from which the information is obtained.
- The date the information was collected and, where feasible, the date the accuracy of the information was last verified.
- Title and contact information for the person to whom the questions regarding the information should be directed.

11. The NYSIC will attach (or ensure that the originating agency has attached) specific labels and descriptive details specified above to information that will be used, accessed, or disseminated. Labels and originating information will clearly indicate any legal restrictions on information sharing based upon information sensitivity or classification.

12. The NYSIC will retain a record of the source of all information sought and collected.

F. Acquiring and Receiving Information

1. Information gathering (acquisition), access, and investigative techniques used by the NYSIC and information-originating agencies are in compliance with and will adhere to applicable regulations and guidelines including, but not limited to:

- 28 CFR Part 23, regarding criminal intelligence information.
- Organisation for Economic Co-operation and Development's (OECD) *Fair Information Practices*.
- Applicable criminal intelligence guidelines under the US Department of Justice's (USDOJ) *National Criminal Intelligence Sharing Plan* (NCISP).
- Applicable relevant constitutional provisions and administrative rules, as well as any other regulations that apply to multijurisdictional intelligence and information sharing (see B-3, Policy Applicability and Legal Compliance).

2. The NYSIC's SAR process provides for vetting to ensure that information is both legally gathered and, where applicable, determined to have a potential terrorism nexus. Field Intelligence Officers (FIOs), law enforcement, and NYSIC staff are trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism.

3. The NYSIC's SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved in activities that have been determined to be consistent with criminal activities associated with terrorism will be documented and shared through the ISE-SAR Reporting initiative. These safeguards are intended to ensure that information that could violate civil rights (e.g., race, culture/ethnicity, religion, national origin, or political association) and civil liberties (e.g. speech, assembly, religious exercise, etc.) will not be intentionally or inadvertently gathered, documented, processed, and shared.

4. Information-gathering techniques used by the NYSIC will be the least intrusive means necessary in the particular circumstances to gather information it is authorized to seek or retain.

5. External agencies that access and share information with the NYSIC are governed by the laws and rules governing those individual agencies, as well as by applicable federal and state laws (see B-3).

6. The NYSIC will seek to 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 their methods are not based on misleading information-gathering practices.

7. The NYSIC will not directly or indirectly seek, receive, accept, or retain information from any individual or information provider that (1) may or may not receive a fee or benefit from providing the information, except as expressly authorized by law or NYSIC policy, or (2) is legally prohibited from obtaining or disclosing the information.

G. Information Quality Assurance

1. The NYSIC will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources of information. NYSIC personnel will take appropriate steps to ensure that information is accurate; current; complete, contextual; and merged with other information about the same individual or organization only when NYSIC Criminal Intelligence and Analysis System (CIAS) Records Merging standards have been met.

2. At the time of retention in the system, the information will be labeled regarding its level of quality (accurate, complete, current, verifiable, and reliable).

3. The NYSIC will investigate, in a timely manner, alleged errors and deficiencies (or refer them to the originating agency) and will correct, delete, or refrain from using protected information found to be erroneous or deficient.

4. The labeling of retained information will be reevaluated when new information is gathered that has an impact on the validity and reliability of previous information.

5. The NYSIC will make every reasonable effort to ensure that information will be corrected, deleted from the system, or not used when the NYSIC learns, through conducting periodic data quality reviews, that the information is erroneous, misleading, obsolete, or otherwise unreliable; the source of the information did not have authority to gather the information or to provide the information; or the source used prohibited means to gather the information, EXCEPT when the source was not acting as the agent of a sworn law enforcement officer.

6. Originating agencies external to the NYSIC are responsible for the quality and accuracy of the data accessed by or provided to the NYSIC. The NYSIC will advise the originating agency's privacy official, if one exists, or the contact person, in writing, if data is alleged, suspected, or found to be inaccurate, incomplete, or out of date.

7. The NYSIC will use timely written or electronic notification to inform recipient agencies when information previously provided to the recipient agency is deleted or changed by the NYSIC. For example, information affecting the rights of an individual that has been determined to be erroneous, outdated, or taken out of context must be corrected.

H. Collection and Analysis

1. Information acquired or received by the NYSIC or accessed from other sources will be analyzed only by selected, approved, and trained individuals who have successfully completed a background check and, if applicable, meet appropriate security clearance levels.

2. Information subject to collection and analysis is defined in Sections E-1 and E-2.

3. Information acquired or received by the NYSIC or accessed from other sources is analyzed according to New York State's priorities and needs, and will be analyzed to:

- Further crime and terrorism prevention, enforce laws, deploy forces, assist prosecution, or meet the objectives and priorities established by the NYSIC, or
- 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 or terrorist activities.

I. Merging Records

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

The set of identifying information sufficient to allow merging will utilize reasonable steps to identify the subject and should include the name (full or partial) and, in most cases, one or more of the following: date of birth; law enforcement or corrections systems identification number; individual identifiers, such as fingerprints, photographs, social security number or other biometrics, such as DNA, retinal scan, or facial recognition.

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

J. Sharing and Disclosure

1. Appropriate credentials, along with electronic user authentication via user name and password, will be used to control information that:

- Specified class(es) of users can view, add, change, delete, or print; and
- Can be disclosed to which individuals and under what circumstances.

2. The NYSIC adheres to national standards for the 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 reporting. For further details, refer to Appendix C: *New York State Intelligence Center (NYSIC) ISE-SAR Privacy, Civil Rights, and Civil Liberties Protection Policy*.

3. Access to or disclosure of records retained by the NYSIC will be provided only to persons within the NYSIC or to other governmental agencies with a "need to know" who are authorized to have access; and only for legitimate law enforcement, public protection, safety, 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. In addition, an audit log will be generated by the NYSIC that details access and dissemination of information.

4. All intelligence products produced under Section H, Collection and Analysis, are subject to supervisory review and Privacy Officer approval, when appropriate, prior to dissemination in order to ensure that they provide appropriate privacy, civil rights, and civil liberties protections.

5. Agencies and individuals external to the NYSIC shall adhere to the third-party rule: Information received from NYSIC must not be disseminated without prior approval from the originator of the information, unless otherwise indicated.

6. Upon approval of the Security Officer, audit record information gathered and retained may be accessed and disseminated for specific purposes to persons authorized by law to have such access. Audit logs will be maintained for five years.

7. Information gathered and records retained by the NYSIC 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, and not exempt from disclosure by law. Such information may be disclosed only in accordance with the law and procedures applicable to the NYSIC for this type of information. An audit log will be kept of all requests and the information disclosed to the public.

8. Information gathered and records retained by the NYSIC will not be:

- Sold, published, exchanged, or disclosed for commercial purposes;
- Disclosed or published without prior notice to the originating agency that such information is subject to redisclosure or publication, unless disclosure is agreed to as part of the normal operations of the agency; or
- Disseminated to persons not authorized to access or use the information.

9. There are several categories of records that will ordinarily not be provided to the public. Determination of whether records should be released will be handled by the NYSIC's Privacy Officer, in conjunction with the New York State Police Records Access Officer and/or Division Counsel at the NYSP Division Headquarters.

- Records that will not be provided to the public include all statutory Freedom of Information Law (FOIL) exemptions outlined in the Article 6 of the Public Officer's Law, §87(2)(a)-(i) (2009).

10. The NYSIC shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information.

K. Redress

K-1 Disclosure

1. Upon satisfactory verification (fingerprints, driver's license or other specified identifying documentation) of his or her identity and subject to the conditions specified in (2), an individual is entitled to know the existence

of and to review the information about him or her that has been collated and retained by the NYSIC. Through the New York State Police – Division Headquarters - Records Access Officer, NYSIC Privacy Officer and Division Counsel's Office, the individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information. As directed by the Records Access Officer, NYSIC Privacy Officer and Division Counsel, NYSIC's response to the request for information will be made within a reasonable time and in a form that is readily intelligible to the individual. A record will be kept of all requests and of what information is disclosed to an individual.

2. As per Article 6 of the Public Officer's Law, §87(2)(e(i, ii, iii, iv)), (f), (g) and (i) the existence, content, and source of the information will not be made available to an individual when:

- Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution (§87 (2) (e(i)(ii));
- Disclosure would endanger the health or safety of an individual, organization, or community (§87 (2) (f));
- The information is in a criminal intelligence system (§87 (2) (e(iv)),(g),(i)); or
- The information relates to victims, juveniles, or other protected classes of information (§87 (2) (e(iii))(f)).

K-2 Complaints and Corrections

1. If an individual has complaints or objections to the accuracy or completeness of information originating from the NYSIC**,** the NYSIC's Privacy Officer, in conjunction with either the NYSP Records Access Officer or Division Counsel's Office, will inform the individual of the procedure for submitting complaints or requesting corrections. A record will be kept of all complaints and requests for correction and the resulting action, if any. The NYSIC Privacy Officer can be reached by contacting the NYSIC at 518-786-2100, or via mail: Attn. Privacy Officer, 630 Columbia Street Ext., Latham, NY, 12110.

2. If an individual has complaints or objections to the accuracy or completeness of information that originates with another agency, the NYSIC Privacy Officer will notify the source agency of the complaint or request for correction, and, if appropriate, ensure that the individual is provided with the source agency's contact information and complaint submission or corrections procedures. A record will be kept of all such complaints and requests for correction and the resulting action taken, if any.

3. If a request for correction of information that has been disclosed is denied by the NYSIC, the originating agency, or an ISE participating agency, reason(s) for denial will be provided to the individual. The individual will also be informed of the appeal process when the NYSIC, originating agency, or ISE participating agency has declined to correct challenged information to his/her satisfaction.

4. If an individual has a complaint with regard to the accuracy or completeness of terrorism-related protected information that: (a) Is exempt from disclosure, and (b) Has been or may be shared through the ISE; and (1) Is held by the NYSIC and (2) Allegedly has resulted in demonstrable harm to the complainant, the NYSIC will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the NYSIC's Privacy Officer. The NYSIC Privacy Officer can be reached by contacting the NYSIC at 518-786-2100, or via mail: Attn. Privacy Officer, 630 Columbia Street Ext., Latham, NY, 12110. 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 NYSIC, the Privacy Officer will notify the originating agency in writing or electronically within 5 business 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 NYSIC 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 NYSIC 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.

5. To delineate protected information shared through the ISE from other data, the NYSIC maintains records of the ISE participating agencies to which the fusion center has access, as well as audit logs, and will maintain originating agency identifiers.

L. Security Safeguards

1. The NYSIC Security Officer – NYSP Lieutenant - will coordinate the protection of the NYSIC's information physical and cyber infrastructure with appropriate NYSP personnel who are specifically trained in these matters.

2. The NYSIC will operate in a secure facility that is protected against external intrusion. The NYSIC will utilize internal and external safeguards against network intrusions. Access to the NYSIC databases from outside the facility will only be allowed via secure networks, using double-factor authentication to verify the identity of personnel.

3. The NYSIC secures tips, leads, and SAR information in a repository system that separates verified data from unverified data.

4. The NYSIC will store information in a manner such that it cannot be added to, modified, accessed, destroyed, or purged except by the originator or by supervisory personnel who have been specifically authorized to take such actions.

5. Access to NYSIC information will be granted only to NYSIC personnel who have been selected, approved, and trained AND whose positions and job duties require such access. Personnel must have successfully completed a background check and, if applicable, retain the appropriate security clearance.

6. Queries made to the NYSIC data applications will be logged into the data system to identify the user initiating the query.

7. The NYSIC's Criminal Intelligence and Analysis System will utilize audit logs to maintain an audit trail for requested, accessed, modified, disseminated, and deleted information.

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

9. The NYSIC will notify any individual about whom personal information was or is reasonably believed to have been breached or obtained by an unauthorized person; access to this information must be demonstrated to cause physical or financial harm or affect the reputation of the individual. 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.

M. Information Retention and Destruction

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

2. When information has no further value or meets the criteria for removal according to the NYSIC's retention and destruction policy, it will be purged, destroyed, and deleted, or returned to the submitting source.

3. The NYSIC will delete information or return it to the source unless it is validated as specified in 28 CFR Part 23.

4. Depending on the relevance of the information, and subject to any specific agreement with the providing agency, notification of proposed destruction may or may not be provided to the source agency per NYSIC discretion.

5. A record of information to be reviewed for retention will be maintained by the NYSIC, 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

N-1 Information System Transparency

1. Regarding information and intelligence collection, the NYSIC's practices are transparent. The NYSIC's privacy policy will be made available to the public via the New York State Police public webpage, http://www.troopers.state.ny.us/Counter_Terrorism/.

2. The NYSIC's Privacy Officer will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberty protections within the NYSIC's information system(s). The NYSIC Privacy Officer can be reached by contacting the NYSIC at 518-786-2100, or via mail: Attn. Privacy Officer, 630 Columbia Street Ext., Latham, NY, 12110.

N-2 Accountability

1. The audit log of queries made to the NYSIC will identify the user initiating the query.

2. The NYSIC will maintain an audit trail of accessed, requested, or disseminated information. An audit trail will be kept for a minimum of 5 years.

3. The NYSIC will provide a copy of this policy to NYSIC personnel and any affiliates and will require written acknowledgement of receipt, along with agreement to comply with the NYSIC Privacy Policy.

4. The NYSIC will adopt and follow procedures and practices by which it can evaluate the compliance of users with system security and privacy. This includes periodic (at least quarterly) system audits. A record of the audits will be maintained by the NYSIC Security Officer.

5. NYSIC authorized users shall report violations of NYSIC policy relating to protected information to the NYSIC Privacy Officer.

6. The NYSIC will regularly conduct random audits and inspections of the information contained in its criminal intelligence system. Periodic data quality reviews will be conducted to systematically review and identify inaccurate, incomplete, improperly merged, or out of date information. Audits will be conducted by a designated New York State Police representative. The NYSP representative has the option of conducting an unannounced random audit at any time, without prior notice to the NYSIC. This audit must protect the confidentiality, sensitivity, and privacy of the NYSIC's criminal intelligence system.

7. The Privacy and Security Officers will conduct an annual Privacy Policy review and update. Specifically, this review focuses upon privacy, civil rights, and civil liberty protections. Changes in applicable law, technology, information systems and public expectations may require updates to the NYSIC Privacy Policy.

8. In addition to annual Policy review, the Privacy Officer will periodically evaluate intelligence product templates and dissemination guidelines to ensure they provide appropriate privacy, civil rights, and civil liberties protections.

9. The NYSIC shall submit to an annual review conducted by its Privacy Officer and the NYSP Internal Affairs Bureau. The NYSIC shall also submit to national-level fusion center audits conducted by the US Department of Homeland Security.

10. Data breaches that may cause harm to any individual must be fully investigated and the affected person(s) and agencies notified (see L.9).

N-3 Enforcement

1. The NYSIC reserves the right to restrict the qualifications and number of personnel having access to NYSIC information and to suspend or withhold service to any personnel violating the privacy policy. The NYSIC reserves the right to deny access to any participating agency user who fails to comply with the applicable restrictions and limitations of the NYSIC's privacy policy.

2. The NYSIC Security and Privacy Officers will, in cooperation with the Director of the NYSIC, move to suspend, demote, transfer, or terminate the person, as permitted by applicable administrative personnel policies; and may refer the matter to the appropriate authorities for criminal prosecution.

O. Training

1. The NYSIC requires the following individuals to participate in annual training programs regarding implementation of and adherence to the privacy, security, civil rights, and civil liberties policies:

- The designated Privacy and Security Officers
- All personnel assigned to the NYSIC
- Personnel providing information technology services to the NYSIC
- Staff from other public agencies or private contractors providing services to the NYSIC.

2. The NYSIC provides special orientation and information sharing training to personnel authorized to share protected information through the Information Sharing Environment (ISE).

3. The NYSIC's Privacy Policy training program covers:

- Purpose of the privacy, including substance and intent;
- Civil rights and civil liberty protection;
- Provisions related to collection, use, analysis, sharing, disclosure, retention, and destruction of information;
- The impact of improper activities associated with infractions upon the NYSIC;
- Mechanisms for reporting violations of the NYSIC privacy protection policy; and
- Penalties for Privacy Policy violation.

References

Baseline Capabilities for State and Major Urban Area Fusion Centers: A Supplement to the Fusion Center Guidelines; September 2008.

Federal Bureau of Investigation (FBI), *Criminal Justice Information Services (CJIS) Division, Privacy Impact Assessment of the Law Enforcement National Data Exchange (N-DEx),* http://foia.fbi.gov/piandex040607.htm

Global Justice Information Sharing Initiative, *Fusion Center Guidelines: Developing and Sharing Intelligence in a New Era – Guidelines for Establishing and Operating Fusion Centers at the Local, State, and Federal Levels* (Washington, DC: Bureau of Justice Assistance, July 2005).

Office of the Director of National Intelligence – *Information Sharing Environment Implementation Plan*, Program Manager – Information Sharing Environment (Washington, DC, 2006).

Office of the Program Manager, Information Sharing Environment (ISE), *Guidelines to Ensure That the Information Privacy and Other Legal Rights of Americans Are Protected in the Development and Use of the Information Sharing Environment (ISE Privacy Guidelines),* www.ise.gov/docs/ise%20privacy%20guidelines%2012-4-06.pdf

Office of the Program Manager, ISE, *An Introduction to the ISE Privacy Guidelines,* www.ise.gov/docs/ise%20privacy%20guidelines%20intro%20-rev.pdf

Office of the Program Manager, ISE, *Privacy and Civil Liberties Implementation Guide for the Information Sharing Environment (ISE),* www.ise.gov/docs/privacy/PrivacyImpGuide_V1.0_20070912.pdf

Organisation for Economic Co-operation and Development *(OECD) Fair Information Practices,* http://it.ojp.gov/documents/OECD_FIPs.pdf

US Department of Justice. *Code of Federal Regulations (CFR), Title 28 (28 CFR)—Judicial Administration, Chapter 1—Part 23—Criminal Intelligence Systems Operating Policies.* http://it.ojp.gov/documents/28CFR_Part_23.PDF

US Department of Justice, *Fusion Center Guidelines: Law Enforcement Intelligence, Public Safety, and the Private Sector, Global Intelligence Working Group,* http://it.ojp.gov/topic.jsp?topic_id=209

US Department of Justice, *National Criminal Intelligence Sharing Plan,* http://www.iir.com/global/products/NCISP_Plan.pdf

US Department of Justice, *Privacy and Civil Liberties Policy Development Guide and Implementation Templates*, Global Justice Information Sharing Initiative's (Global) Privacy and Information Quality Working Group.

US Department of Justice, *Privacy, Civil Rights, and Civil Liberties Policy Templates for Justice Information Systems,* Global Privacy & Information Quality Working Group & the Justice Management Institute, http://it.ojp.gov/documents/Privacy_Civil_Rights_and_Civil_Liberties_Policy_Templates.pdf

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-lonely and read/write access.

With regard to 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—Agency refers to the NYSP and all agencies that access, contribute, and share information in the NYSIC's justice information system.

Audit Trail—Audit trail is a generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail – what commands were issued to the system, what records and files were accessed or modified, etc.

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—Authentication is 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.

Center—Center refers to the NYSIC and all participating state agencies of the NYSIC.

Civil Liberties—Civil Liberties are fundamental individual rights, such as freedom of speech, press, or religion; due process 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, obligation 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—Confidentiality is closely related to privacy but is not identical. It refers to the obligations of individuals and institutions to use information under their control appropriately once it has been disclosed to them. One observes rules of confidentiality out of respect for and to protect and preserve the privacy of others. See Privacy.

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 and Analysis System (CIAS)—The NYSIC's intelligence and case management database system.

Criminal Intelligence Information or Data—Information deemed relevant to the identification of and the criminal activity engaged in by an individual who or organization that is reasonably suspected of involvement in criminal acts. The record is maintained in a criminal intelligence system per 28CFR Part 23. Reasonable suspicion applies to the information.

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

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

Director—The Director of the NYSIC assumes primary responsibility for the daily operation of the NYSIC, its personnel, and associated data and systems.

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

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

Fair Information Practices—The Fair Information Practices (FIPs) are contained within the 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 FIPS 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) related 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 attack.

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 given and family name, date of birth, and address. An organization's identification process consists of the acquisition of the relevant identifying information.

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

Information Sharing Environment (ISE) 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).

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

Intelligence-Led Policing (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.

Law—As used by this policy, law includes any local, state, or federal 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.

Logs—Logs are a necessary part of an adequate security system because they are needed to ensure that data is properly tracked and 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.

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.

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—Any agency or organization with personnel assigned to work at the NYSIC. Each participating agency must have a signed memorandum of understanding (MOU) on file with the NYSIC, which authorizes the agency access to receive and use center information and/or intelligence databases and resources for lawful purposes through its authorized individual users.

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

- 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, Automated Integrated Fingerprint Identification System [AIFIS] 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 locations(s) or place(s) (including geographic information systems [GIS] locations, electronic bracelet monitoring information, etc.).

Persons—For the purposes of this privacy policy, the term "persons" is not limited to is United States citizens, but includes all individuals regardless of residency status.

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

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

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

Privacy Officer—Appointed by the Director of the NYSIC, this individual is responsible for ensuring the Center's compliance with and enforcement of all applicable privacy laws, federal and state Constitutions, rules, regulations, and policies.

Protected Information— For the purposes of this NYSIC privacy policy, protected information is information about persons, and is subject to information privacy or other legal protections under:

- the US Constitution
- laws of the United States
- state and tribal constitutions
- state, local, and tribal laws, ordinances, and codes.

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 agency's center's information;
- Media organizations; and
- Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the agency.

Public does *not* include:

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

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

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.

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.

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—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.

Security Officer—Appointed by the Director of the NYSIC, this individual is responsible for ensuring that all information and intelligence records are properly stored and secured at all times.

Source Agency—Source agency refers to the agency or organizational entity that originates 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:

1. Storage is frequently used to mean the devices and data connected to the computer through input/output operations - that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-computer storage. This meaning is probably more common in the IT industry than meaning 2.

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

Suspicious Activity—Suspicious activity is defined as "reported or observed activity and/or behavior that, based on an officer's training and experience, is believe to be indicative of intelligence gathering or preoperational planning related to terrorism, criminal or other illicit intention." Examples of suspicious activity include surveillance, photography of facilities, site breach or physical intrusion, cyberattacks, testing of security, etc.

Suspicious Activity Report (SAR)—Official documentation of observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity. Suspicious activity report (SAR) information offers a standardized means for feeding information repositories or data analysis tools. Patterns identified during SAR information analysis may be investigated in coordination with the reporting agency and, if applicable, a state or regional fusion center. SAR

information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor is it designed to support interagency calls for service.

Terrorism Information—Consistent with Section 1016(a)(4) of 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 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 has some suspicion or is based on a level of suspicion that is less than "reasonable suspicion," but without further inquiry or analysis, it is unknown whether the information is accurate or useful. Tips and leads information falls between being of 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.

Appendix B – Privacy Policy - Applicable Laws

- US CONST. and US CONST. Amend. I-XXVII
- The Privacy Act of 1974 (5 USC 552a)
- US Executive Order 12958 "Classified National Security Information"
- USDOJ Criminal Intelligence Systems Operating Policies, 28 CFR Part 23 (1998)
- N.Y. State Penal Law, Part III, Title J - Article 156
- N.Y. Public Officer's Law, Articles 6 and 6-A
- N.Y. Public Officer's Law, Chapter 47 of the Consolidated Laws; Article 6, Section 87 (a), (b), (e), (f) and (g)

New York State Penal Law

Part III Specific Offenses; Title J. Offenses Involving Theft - Article 156. Offenses Involving Computers

s 156.10 Computer trespass

A person is guilty of computer trespass when he or she knowingly uses, causes to be used, or accesses a computer, computer service, or computer network without authorization and:

1. he or she does so with an intent to commit or attempt to commit or further the commission of any felony; or

2. he or she thereby knowingly gains access to computer material.

Computer trespass is a class E felony**.**

s 156.05 Unauthorized use of a computer

A person is guilty of unauthorized use of a computer when he knowingly uses or causes to be used a computer or computer service without authorization and the computer utilized is equipped or programmed with any device or coding system, a function of which is to prevent the unauthorized use of said computer or computer system.

Unauthorized use of a computer is a class A misdemeanor.

New York State Public Officer's Law

Article 6. Freedom of Information Law

s 87. Access to agency records

1. (a) Within sixty days after the effective date of this article, the governing body of each public corporation shall promulgate uniform rules and regulations for all agencies in such public corporation pursuant to such

general rules and regulations as may be promulgated by the committee on open government in conformity with the provisions of this article, pertaining to the administration of this article.

(b) Each agency shall promulgate rules and regulations, in conformity with this article and applicable rules and regulations promulgated pursuant to the provisions of paragraph (a) of this subdivision, and pursuant to such general rules and regulations as may be promulgated by the committee on open government in conformity with the provisions of this article, pertaining to the availability of records and procedures to be followed, including, but not limited to:

i. the times and places such records are available;
ii. the persons from whom such records may be obtained, and
iii. the fees for copies of records which shall not exceed twenty-five cents per photocopy not in excess of nine inches by fourteen inches, or the actual cost of reproducing any other record in accordance with the provisions of paragraph (c) of this subdivision, except when a different fee is otherwise prescribed by statute.

(c) In determining the actual cost of reproducing a record, an agency may include only:

i. an amount equal to the hourly salary attributed to the lowest paid agency employee who has the necessary skill required to prepare a copy of the requested record;
ii. the actual cost of the storage devices or media provided to the person making the request in complying with such request;
iii. the actual cost to the agency of engaging an outside professional service to prepare a copy of a record, but only when an agency's information technology equipment is inadequate to prepare a copy, if such service is used to prepare the copy; and
iv. preparing a copy shall not include search time or administrative costs, and no fee shall be charged unless at least two hours of agency employee time is needed to prepare a copy of the record requested. A person requesting a record shall be informed of the estimated cost of preparing a copy of the record if more than two hours of an agency employee's time is needed, or if an outside professional service would be retained to prepare a copy of the record.

2. Each agency shall, in accordance with its published rules, make available for public inspection and copying all records, except that such agency may deny access to records or portions thereof that:

(a) are specifically exempted from disclosure by state or federal statute;

(b) if disclosed would constitute an unwarranted invasion of personal privacy under the provisions of subdivision two of section eighty-nine of this article;

(c) if disclosed would impair present or imminent contract awards or collective bargaining negotiations;

(d) are trade secrets or are submitted to an agency by a commercial enterprise or derived from information obtained from a commercial enterprise and which if disclosed would cause substantial injury to the competitive position of the subject enterprise;

(e) are compiled for law enforcement purposes and which, if disclosed, would:

i. interfere with law enforcement investigations or judicial proceedings;
ii. deprive a person of a right to a fair trial or impartial adjudication;

iii. identify a confidential source or disclose confidential information relating to a criminal investigation; or
iv. reveal criminal investigative techniques or procedures, except routine techniques and procedures;

(f) if disclosed could endanger the life or safety of any person;

(g) are inter-agency or intra-agency materials which are not:

i. statistical or factual tabulations or data;
ii. instructions to staff that affect the public;
iii. final agency policy or determinations;
iv. external audits, including but not limited to audits performed by the comptroller and the federal government; or

(h) are examination questions or answers which are requested prior to the final administration of such questions.

(i) if disclosed, would jeopardize an agency's capacity to guarantee the security of its information technology assets, such assets encompassing both electronic information systems and infrastructures; or

(j) [Eff. until Dec. 1, 2009, pursuant to L.1988, c. 746, s 17.] are photographs, microphotographs, videotape or other recorded images prepared under authority of section eleven hundred eleven-a of the vehicle and traffic law.

3. Each agency shall maintain:

(a) a record of the final vote of each member in every agency proceeding in which the member votes;

(b) a record setting forth the name, public office address, title and salary of every officer or employee of the agency; and

(c) a reasonably detailed current list by subject matter of all records in the possession of the agency, whether or not available under this article. Each agency shall update its subject matter list annually, and the date of the most recent update shall be conspicuously indicated on the list. Each state agency as defined in subdivision four of this section that maintains a website shall post its current list on its website and such posting shall be linked to the website of the committee on open government. Any such agency that does not maintain a website shall arrange to have its list posted on the website of the committee on open government.

4. (a) Each state agency which maintains records containing trade secrets, to which access may be denied pursuant to paragraph (d) of subdivision two of this section, shall promulgate regulations in conformity with the provisions of subdivision five of section eighty-nine of this article pertaining to such records, including, but not limited to the following:

(1) the manner of identifying the records or parts;

(2) the manner of identifying persons within the agency to whose custody the records or parts will be charged and for whose inspection and study the records will be made available;

(3) the manner of safeguarding against any unauthorized access to the records.

(b) As used in this subdivision the term "agency" or "state agency" means only a state department, board, bureau, division, council or office and any public corporation the majority of whose members are appointed by the governor.

(c) Each state agency that maintains a website shall post information related to this article and article six-A of this chapter on its website. Such information shall include, at a minimum, contact information for the persons from whom records of the agency may be obtained, the times and places such records are available for inspection and copying, and information on how to request records in person, by mail, and, if the agency accepts requests for records electronically, by e-mail. This posting shall be linked to the website of the committee on open government.

5. (a) An agency shall provide records on the medium requested by a person, if the agency can reasonably make such copy or have such copy made by engaging an outside professional service. Records provided in a computer format shall not be encrypted.

(b) No agency shall enter into or renew a contract for the creation or maintenance of records if such contract impairs the right of the public to inspect or copy the agency's records.

Article 6-A. Personal Privacy Protection Law (Refs & Annos)

s 95. Access to records

(1)(a) Each agency subject to the provisions of this article, within five business days of the receipt of a written request from a data subject for a record reasonably described pertaining to that data subject, shall make such record available to the data subject, deny such request in whole or in part and provide the reasons therefore in writing, or furnish a written acknowledgement of the receipt of such request and a statement of the approximate date when such request will be granted or denied, which date shall not exceed thirty days from the date of the acknowledgement.

(b) An agency shall not be required to provide a data subject with access to a record pursuant to this section if:

(i) the agency does not have the possession of such record;
(ii) such record cannot be retrieved by use of the data subject's description thereof, or by use of the name or other identifier of the data subject, without extraordinary search methods being employed by the agency; or
(iii) access to such record is not required to be provided pursuant to subdivision five, six or seven of this section.

(c) Upon payment of, or offer to pay, the fee prescribed by section eighty-seven of this chapter, the agency shall provide a copy of the record requested and certify to the correctness of such copy if so requested. The record shall be made available in a printed form without any codes or symbols, unless accompanied by a document fully explaining such codes or symbols. Upon a data subject's voluntary request the agency shall permit a person of the data subject's choosing to accompany the data subject when reviewing and obtaining a copy of a record, provided that the agency may require the data subject to furnish a written statement authorizing discussion of the record in the accompanying person's presence.

(2) Each agency shall, within thirty business days of receipt of a written request from a data subject for correction or amendment of a record or personal information, reasonably described, pertaining to that data subject, which he or she believes is not accurate, relevant, timely or complete, either:

(a) make the correction or amendment in whole or in part, and inform the data subject that upon his or her request such correction or amendment will be provided to any or all persons or governmental units to which the record or personal information has been or is disclosed, pursuant to paragraph (c) of subdivision three of section ninety-four of this article; or

(b) inform the data subject of its refusal to correct or amend the record and its reasons therefor [sic].

(3) Any data subject whose request under subdivision one or two of this section is denied in whole or in part may, within thirty business days, appeal such denial in writing to the head, chief executive or governing body of the agency, or the person designated as the reviewing official by such head, chief executive or governing body. Such official shall within seven business days of the receipt of an appeal concerning denial of access, or within thirty business days of the receipt of an appeal concerning denial of correction or amendment, either provide access to or correction or amendment of the record sought and inform the data subject that, upon his or her request, such correction or amendment will be provided to any or all persons or governmental units to which the record or personal information has been or is disclosed, pursuant to paragraph (c) of subdivision three of section ninety-four of this article, or fully explain in writing to the data subject the factual and statutory reasons for further denial and inform the data subject of his or her right to thereupon seek judicial review of the agency's determination under section ninety-seven of this article. Each agency shall immediately forward to the committee a copy of such appeal, the determination thereof and the reasons therefore.

(4) If correction or amendment of a record or personal information is denied in whole or in part upon appeal, the agency shall inform the data subject of the right to file with the agency a statement of reasonable length setting forth the reasons for disagreement with the agency's determination and that, upon request, his or her statement of disagreement will be provided to any or all persons or governmental units to which the record has been or is disclosed, pursuant to paragraph (c) of subdivision three of section ninety-four of this article. With respect to any personal information about which a data subject has filed a statement of disagreement, the agency shall clearly note any portions of the record which are disputed, and shall attach the data subject's statement of disagreement as part of the record. When providing the data subject's statement of disagreement to other persons or governmental units pursuant to paragraph (c) of subdivision three of section ninety-four of this article, the agency may, if it deems appropriate, also include in the record a concise statement of the agency's reasons for not making the requested amendment.

(5)(a) Any agency which may not otherwise exempt personal information from the operation of this section may do so, unless access by the data subject is otherwise authorized or required by law, if such information is compiled for law enforcement purposes and would, if disclosed:

(i) interfere with law enforcement investigations or judicial proceedings;
(ii) deprive a person of a right to a fair trial or impartial adjudication;
(iii) identify a confidential source or disclose confidential information relating to a criminal investigation; or
(iv) reveal criminal investigative techniques or procedures, except routine techniques and procedures.

(b) When providing the data subject with access to information described in paragraph (b) of subdivision seven of section ninety-four of this article, an agency may withhold the identity of a source who furnished said information under an express promise that his or her identity would be held in confidence.

(6) Nothing in this section shall require an agency to provide a data subject with access to:

(a) personal information to which he or she is specifically prohibited by statute from gaining access;

(b) patient records concerning mental disability or medical records where such access is not otherwise required by law;

(c) personal information pertaining to the incarceration of an inmate at a state correctional facility which is evaluative in nature or which, if such access was provided, could endanger the life or safety of any person, unless such access is otherwise permitted by law or by court order;

(d) attorney's work product or material prepared for litigation before judicial, quasi-judicial or administrative tribunals, as described in subdivisions (c) and (d) of section three thousand one hundred one of the civil practice law and rules, except pursuant to statute, subpoena issued in the course of a criminal action or proceeding, court ordered or grand jury subpoena, search warrant or other court ordered disclosure.

(7) This section shall not apply to public safety agency records.

(8) Nothing in this section shall limit, restrict, abrogate or deny any right a person may otherwise have including rights granted pursuant to the state or federal constitution, law or court order.

Article 6-A. Personal Privacy Protection Law

s 96. Disclosure of records

(1) No agency may disclose any record or personal information unless such disclosure is:

(a) pursuant to a written request by or the voluntary written consent of the data subject, provided that such request or consent by its terms limits and specifically describes:

(i) the personal information which is requested to be disclosed;
(ii) the person or entity to whom such personal information is requested to be disclosed; and
(iii) the uses which will be made of such personal information by the person or entity receiving it; or

(b) to those officers and employees of, and to those who contract with, the agency that maintains the record if such disclosure is necessary to the performance of their official duties pursuant to a purpose of the agency required to be accomplished by statute or executive order or necessary to operate a program specifically authorized by law; or

(c) subject to disclosure under article six of this chapter, unless disclosure of such information would constitute an unwarranted invasion of personal privacy as defined in paragraph (a) of subdivision two of section eighty-nine of this chapter; or

(d) to officers or employees of another governmental unit if each category of information sought to be disclosed is necessary for the receiving governmental unit to operate a program specifically authorized by statute and if the use for which the information is requested is not relevant to the purpose for which it was collected; or

(e) for a routine use, as defined in subdivision ten of section ninety-two of this article; or

(f) specifically authorized by statute or federal rule or regulation; or

(g) to the bureau of the census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of Title XIII of the United States Code; or

(h) to a person who has provided the agency with advance written assurance that the record will be used solely for the purpose of statistical research or reporting, but only if it is to be transferred in a form that does not reveal the identity of any data subject; or

(i) pursuant to a showing of compelling circumstances affecting the health or safety of a data subject, if upon such disclosure notification is transmitted to the data subject at his or her last known address; or

(j) to the state archives as a record which has sufficient historical or other value to warrant its continued preservation by the state or for evaluation by the state archivist or his or her designee to determine whether the record has such value; or

(k) to any person pursuant to a court ordered subpoena or other compulsory legal process; or

(l) for inclusion in a public safety agency record or to any governmental unit or component thereof which performs as one of its principal functions any activity pertaining to the enforcement of criminal laws, provided that, such record is reasonably described and is requested solely for a law enforcement function; or

(m) pursuant to a search warrant; or

(n) to officers or employees of another agency if the record sought to be disclosed is necessary for the receiving agency to comply with the mandate of an executive order, but only if such records are to be used only for statistical research, evaluation or reporting and are not used in making any determination about a data subject.

(2) Nothing in this section shall require disclosure of:

(a) personal information which is otherwise prohibited by law from being disclosed;

(b) patient records concerning mental disability or medical records where such disclosure is not otherwise required by law;

(c) personal information pertaining to the incarceration of an inmate at a state correctional facility which is evaluative in nature or which, if disclosed, could endanger the life or safety of any person, unless such disclosure is otherwise permitted by law;

(d) attorney's work product or material prepared for litigation before judicial, quasi-judicial or administrative tribunals, as described in subdivisions (c) and (d) of section three thousand one hundred one of the civil practice law and rules, except pursuant to statute, subpoena issued in the course of a criminal action or proceeding, court ordered or grand jury subpoena, search warrant or other court ordered disclosure.

Appendix C –NYSIC ISE-SAR Privacy, Civil Rights, and Civil Liberties Protection Policy

New York State Intelligence Center (NYSIC)
ISE-SAR Privacy, Civil Rights, and Civil Liberties Protection Policy

A. Purpose Statement

1. The purpose of the ISE-SAR Evaluation Environment Initiative (hereafter "EE Initiative") Privacy, Civil Rights, and Civil Liberties Protection Policy (hereafter "Privacy and CR/CL Policy") is to promote the New York State Intelligence Center (hereafter "NYSIC," "submitting agency," or "source agency"), and user agency (hereafter collectively referred to as "participating agencies" or "participants") conduct under the EE Initiative that complies with applicable federal, state, local, and tribal laws, regulations, and policies and assists participants in:

   - Ensuring individual privacy, civil rights, civil liberties, and other protected interests;
   - Increasing public safety and improving national security;
   - Protecting the integrity of systems for the observation and reporting of terrorism-related criminal activity and information;
   - Encouraging individuals or community groups to trust and cooperate with the justice system;
   - Promoting governmental legitimacy and accountability; and
   - Making the most effective use of public resources allocated to public safety agencies.

   NOTE: In its practice and for the purposes of this policy, the NYSIC is both the source agency and the submitting agency.

B. Policy Applicability and Legal Compliance

1. All participating NYSIC personnel, including personnel providing information technology services to the NYSIC, private contractors, and other authorized participants will comply with applicable provisions of the NYSIC's Privacy and CR/CL Policy concerning personal information, including:
   - SAR information the NYSIC documents and collects; and
   - The ISE-SAR information identified, submitted to the Shared Space, and accessed by or disclosed to NYSIC personnel.

2. The NYSIC will provide a printed copy of its Privacy and CR/CL Policy to all NYSIC personnel, nonagency personnel who provide services to the NYSIC, and NYSIC authorized users and will require both a written acknowledgement of receipt of this policy and a written agreement to comply with applicable provisions of this policy.

3. All NYSIC personnel, participating agency personnel, personnel providing information technology services to the agency, private contractors, and other authorized users shall comply with applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to: the U.S. Constitution and state, local, and federal privacy, civil rights, civil liberties, legal requirements applicable to the NYSIC and/or other participating agencies.

New York State Police sworn Members must comply with New York State Police Administrative Manual Regulation 8 Section F, specifically Regulation 8F1, 8F7 and 8F8; civilian employees must comply with New York State Police Civilian Employee Manual section 2M. Refer also to Appendix B – New York State Laws.

C. Governance and Oversight

1. The Director of the NYSIC will have primary responsibility for: operating the NYSIC, ISE-SAR information system operations, and coordinating personnel involved in the EE Initiative; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing or disclosure of SAR and ISE-SAR information; and enforcing the provisions of this policy.

2. The NYSIC's participation in the EE Initiative will be guided by a trained Privacy Officer who is appointed by the NYSIC Director to assist in enforcing the provisions of this policy and who, in addition to other responsibilities, will receive reports regarding alleged errors and violations of the provisions of this policy.

D. Terms and Definitions

1. The primary terms and definitions used in this privacy policy are set forth in Appendix A, Terms and Definitions.

E. Information

1. The NYSIC will seek or retain information that it has determined constitutes "suspicious activity" and which:
   - Is based on (a) a criminal predicate or (b) a possible threat to public safety, including potential terrorism-related conduct; and
   - Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; or the prevention of crime; and
   - The NYSIC assures was acquired in accordance with agency policy and in a lawful manner.

2. The NYSIC agrees not to document and collect SAR information and the NYSIC will not retain SAR or ISE-SAR information about any individual that was gathered solely on the basis of that individual's religious, political, or social views or activities; participation in a particular noncriminal organization or lawful event; or race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation.

3. Upon receipt of tip, lead, or other data resulting in the documentation of a SAR, designated NYSIC personnel will:
   - Personally review and vet the tip, lead, or other data and provide the two-step assessment set forth in the ISE-SAR Functional Standard to determine whether the information qualifies as an ISE-SAR;
   - Enter the information following IEPD standards and code conventions to the extent feasible;
   - Provide appropriate labels as required under E.5 and E.6 below;
   - Submit (post) the ISE-SAR to the NYSIC's shared space; and
   - Notify the law enforcement agency submitting the tip, lead, or other data that an ISE-SAR has been submitted to the shared space.

4. The NYSIC will ensure that certain basic and special descriptive information is entered and electronically associated with ISE-SAR information, including:
   - The name of the law enforcement agency submitting a tip, lead, or other data that results in an ISE-SAR submission by the NYSIC ;
   - The date the information was submitted;
   - The point-of-contact information for SAR-related data; and
   - Information that reflects any special laws, rules, or policies regarding access, use, and disclosure.

5. Information provided in the ISE-SAR shall indicate, to the maximum extent feasible and consistent with the Information Sharing Environment (ISE) Functional Standard for Suspicious Activity Reporting (SAR) Version 1.0 (ISE-FS-200):

- The nature of the source: anonymous tip, confidential source, trained interviewer or investigator, written statement (victim, witness, other), private sector, or other source; and
- Confidence, including:
  The reliability of the source of the tip, lead, or other data:
    - reliable – the source has been determined to be reliable;
    - unreliable – the reliability of the source is doubtful or has been determined to be unreliable;
    - unknown – the reliability of the source cannot be judged or has not as yet been assessed; and

  The validity of the content:
    - confirmed – information has been corroborated by an investigator or other reliable source;
    - doubtful – the information is of questionable credibility but cannot be discounted;
    - cannot be judged – the information cannot be confirmed.
- Due diligence will be exercised in determining tip, lead, or other data source reliability and content validity. Information determined to be unfounded will be purged from the shared space.
- Unless otherwise indicated by the submitting agency, source reliability is deemed to be "unknown" and content validity "cannot be judged." In such case, users must independently confirm source reliability and content validity with the source or submitting agency or validate it through their own investigation.

6. At the time a decision is made to post ISE-SAR information to the shared space, NYSIC personnel will ensure that the ISE-SAR information is labeled, to the maximum extent feasible and consistent with the ISE-SAR FS, to reflect any limitations on disclosure based on sensitivity of disclosure (dissemination description code), in order to:
   - Protect an individual's right of privacy, civil rights, and civil liberties;
   - Protect confidential sources and police undercover techniques and methods;
   - Not interfere with or compromise pending criminal investigations; and
   - Provide any legally required protection based on an 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.

7. The NYSIC will share ISE-SAR information with authorized non-fusion center agencies and individuals only in accordance with established NYSIC policy and procedure.

8. The NYSIC will ensure that ISE-SAR information in the shared space that is not verified (confirmed) will be subject to continuing assessment for confidence by subjecting it to an evaluation or screening process to confirm its credibility and value or categorize the information as unfounded or uncorroborated. If subsequent attempts to validate the information confirm its validity or are unsuccessful, the information in the shared space will be updated (replaced) to so indicate. Information determined to be unfounded will be purged from the shared space.

9. The NYSIC will incorporate the gathering, processing, reporting, analyzing, and sharing of SAR and ISE-SAR information (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 the privacy, civil rights, and civil liberties of individuals.

10. Notice will be provided through data field labels or narrative information to enable authorized users to determine the nature of the protected information in the shared space and how to handle the information in

accordance with applicable legal requirements, including any restrictions based on information security or classification.

F. Acquiring and Receiving Information

1. Information acquisition and investigative techniques used by law enforcement agencies reporting tips, leads or data resulting in an ISE-SAR submission by the NYSIC must comply with and adhere to applicable law, regulations and guidelines, including, where applicable, U.S. and state constitutional provisions, applicable federal and state law provisions, local ordinances, and regulations.

2. Law enforcement officers and other personnel at agencies who report tips, leads or other data to the NYSIC that may result in an ISE-SAR submission have been trained to recognize behavior that is indicative of criminal activity related to terrorism.

3. When a choice of investigative techniques is available, information documented as a SAR or ISE-SAR should be acquired or investigated using the least intrusive feasible means, taking into account such factors as the effect on individuals' privacy and potential damage to reputation.

4. Access to and use of ISE-SAR information is governed by the U.S. Constitution, the state constitution, applicable federal and state laws and local ordinances, and PM-ISE policy guidance applicable to the ISE-SAR EE initiative.

G. Information Quality Assurance

1. The NYSIC will ensure that law enforcement agencies reporting tips, lead, or other data resulting in an ISE-SAR submission assume primary responsibility for the quality and accuracy of the information documented by the NYSIC. The NYSIC will advise the appropriate contact person in the agency submitting the tip, lead, or other data resulting in an ISE-SAR submission in writing (this would include electronic notification) if SAR information received from the reporting agency is alleged, suspected, or found to be erroneous or deficient.

2. The NYSIC will make every reasonable effort to ensure that tips, leads, or other data reported and ISE-SAR information retained and posted to the shared space is derived from dependable and trustworthy partner law enforcement agencies and is as accurate, current, and complete as possible.

3. At the time of posting to the shared space, ISE-SAR information will be labeled according to the level of confidence in the information (source reliability and content validity) to the maximum extent feasible.

4. The labeling of ISE-SAR information will be periodically evaluated and updated in the shared space when new information is acquired that has an impact on confidence in the information.

5. Alleged errors or deficiencies (misleading, obsolete, or otherwise unreliable) in ISE-SAR information will be investigated in a timely manner and any needed corrections to or deletions made to such information in the shared space.

6. ISE-SAR information will be removed from the shared space if it is determined that a law enforcement agency providing the tip, lead, or other or data resulting in an ISE-SAR submission did not have authority to acquire the original information, used prohibited means to acquire it, or did not have authority to provide it to the NYSIC or if the information is subject to an expungement order in a state or federal court that is enforceable under state law or policy.

7. The NYSIC will provide written notice (this would include electronic notification) to the law enforcement agency that provided the information resulting in an ISE-SAR submission, and to any user agency that has accessed the ISE-SAR information posted to the shared space, when ISE-SAR information posted to the shared space by the NYSIC is corrected or removed from the shared space by the NYSIC because it is erroneous or deficient such that the rights of an individual may be affected.

H. Analysis

1. ISE-SAR Information posted by the NYSIC to the shared space or accessed from the shared spaces under the EE Initiative will be analyzed for intelligence purposes only by qualified NYSIC personnel who have successfully completed a background check and any applicable security clearance and have been selected, approved, and trained accordingly (including training on the implementation of this policy). These personnel shall share ISE-SAR information only through authorized analytical products.

2. ISE-SAR information is analyzed according to priorities and needs, including analysis to:
   - Further terrorism prevention, investigation, force deployment, or prosecution objectives and priorities established by the NYSIC, and
   - Provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in terrorism-related activities.

I. Sharing and Disclosure

1. Credentialed, role-based access criteria will be used, as appropriate, to determine which system users will be authorized to view privacy fields in ISE-SAR information in response to queries made through a federated ISE-SAR search.

2. Unless an exception is expressly approved by the PM-ISE, the NYSIC will adhere to the Functional Standard for the ISE-SAR process, including the use of the ISE-SAR IEPD reporting format, EE Initiative approved data collection codes, and ISE-SAR information sharing and disclosure business rules.

3. ISE-SAR information retained by the NYSIC and entered into the NYSIC's shared space will be accessed by or disseminated only to persons within the NYSIC or, as expressly approved by PM-ISE, users who are authorized to have access and need the information **for specific purposes authorized by law**. Access and disclosure of personal information will only be allowed to agencies and individual users for legitimate law enforcement and public protection purposes and only for the performance of official duties in accordance with law.

4. ISE-SAR information posted to the shared space by the NYSIC may be 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 NYSIC mission and is not exempt from disclosure by law. Such information may be disclosed only in accordance with the law and procedures applicable to the NYSIC for this type of information. The applicable provisions of law requiring disclosure are identified in Appendix B – New York State Laws – Public Officer's Law.

5. ISE-SAR information **will not be provided** to the public if, pursuant to applicable law, it is:
   - Required to be kept confidential or exempt from disclosure;
   - Classified as investigatory records and exempt from disclosure;
   - Protected federal, state, or tribal records originated and controlled by the source agency that cannot be shared without permission; or
   - A violation of an authorized nondisclosure agreement.

Refer to appendix B – New York State Laws – Public Officer's Law Article 6 s87.

6. The NYSIC will not confirm the existence or nonexistence of ISE-SAR information to any person, organization, or other entity not otherwise entitled to receive the information.

J. Disclosure and Correction/Redress

J.1. Mandatory Disclosure and Correction – See Appendix B – New York State Laws – Public Officer's Law Article 6 s87, Access to Agency Records.

1. Upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity and subject to the conditions specified in 2., below, an individual who is entitled to know the existence of and to review the information about him or her that has been gathered and retained by the NYSIC may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information. The NYSIC's response to the request for information will be made within a reasonable time and in a form that is readily intelligible to the individual. A record will be kept of all requests and of what information is disclosed to an individual.

2. The existence, content, and source of the information will not be made available to an individual when:
   - Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution;
   - Disclosure would endanger the health or safety of an individual, organization, or community; or
   - The NYSIC or user agency did not originate, or does not otherwise have a right to disclose, the information: or
   - If disclosure is otherwise exempted pursuant to the New York State Public Officer's Law Article 6 s87. See Appendix B.

3. The individual to whom information has been disclosed will be given reasons if requests for correction(s) are denied by the NYSIC or the source agency. The individual will also be informed of the procedure for appeal when the NYSIC has declined to correct challenged information to the satisfaction of the individual to whom the information relates.

J.2. Redress (Complaint and correction when no right to disclosure)

1. If an individual has complaints or objections to the accuracy or completeness of ISE-SAR information about him or her that is alleged to be held by the NYSIC, the NYSIC, as appropriate, will inform the individual of the procedure for submitting complaints or requesting corrections. A record will be kept of all complaints and requests for corrections and the resulting action, if any.

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

K. Security Safeguards

1. A Lieutenant assigned to the Criminal Intelligence Section is designated and trained to serve as the NYSIC security officer for the EE Initiative.

2. The NYSIC operates in a secure facility protecting it from external intrusion. The NYSIC will utilize secure internal and external safeguards against network intrusions of ISE-SAR information. Access to the NYSIC's ISE-SAR shared space from outside the facility will be allowed only over secure networks.

3. The NYSIC will secure ISE-SAR information in the NYSIC's shared space in a manner such that it cannot be added to, modified, accessed, destroyed, or purged except by NYSIC personnel authorized to take such actions.

4. Access to ISE-SAR information will be granted only to NYSIC personnel whose positions and job duties require such access; who have successfully completed a background check and any applicable security clearance and who have been selected, approved, and trained accordingly.

5. The NYSIC will, in the event of a data security breach, consider notifying an individual about whom personal information was or is reasonably believed to have been compromised or obtained by an unauthorized person and access to which threatens physical, reputational, or financial harm to the person. Any 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 breach or any measures necessary to determine the scope of the breach and, if necessary, to restore the integrity of the system.

L. Information Retention and Destruction

1. The NYSIC will ensure that all ISE-SAR information is reviewed for record retention (validation or purge) in accordance with the time period specified in NYSIC policy, as applicable. A record entered by NYSIC into the shared space will be maintained for a maximum of 5 years, at which time the record will be reviewed and a determination made to either validate the record for an additional 5 year period, or purge the record from the system.

2. The NYSIC will retain ISE-SAR information in the shared space for a maximum of 90 days to permit the information to be validated or refuted, its credibility and value to be reassessed, and a disposition label assigned.

3. When ISE-SAR information has no further value or meets the NYSIC's criteria for purge according to applicable law or policy, the entire record will be purged.

4. There are no New York State Laws prescribing notification procedures prior to information purging. There will be no notification provided on information purged by the NYSIC

M. Transparency, Accountability, and Enforcement

M.1. Information System Transparency

1. The NYSIC will be open with the public in regard to the process for reporting tips, leads, and other information, documenting SAR information, and processing SARs to identify ISE-SAR information. The NYSIC will make the NYSIC's EE Initiative Privacy Policy available upon request.

2. The NYSIC's Privacy Officer will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections relating to ISE-SAR information.

M.2. Accountability

1. The audit log of queries for ISE-SAR information will identify the user initiating the query.

2. The NYSIC will have access to an audit trail of inquiries to the shared spaces.

3. The NYSIC will adopt and follow procedures and practices to evaluate the compliance of its authorized users with ISE-SAR information policy and applicable law. This will include periodic and random audits of

logged access to the shared spaces in accordance with EE Initiative policy. A record of the audits will be maintained by the Security Officer of the agency.

4. NYSIC personnel shall report violations or suspected violations of the NYSIC's ISE-SAR EE Initiative privacy policy to the NYSIC's Privacy Officer.

5. The NYSIC will conduct periodic audit and inspection of the information contained in its ISE-SAR shared space. The audit will be conducted by NYSIC staff or an independent auditor, as provided by EE Initiative policy. This audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the ISE-SAR information maintained by the NYSIC in the shared space and any related documentation.

6. The NYSIC's appointed and trained Privacy Officer or other expert individual or group designated by the NYSIC will periodically review the NYSIC's EE Initiative Privacy Policy and the NYSIC will make appropriate changes in response to changes in applicable law.

M.3. Enforcement

1. The NYSIC reserves the right to restrict the qualifications and number of user agencies and authorized user agency personnel that it certifies for access to ISE-SAR information and to suspend or withhold service to any of its user agencies or authorized user agency personnel violating this privacy policy. The NYSIC further reserves the right to deny access or participation in the EE Initiative to its participating agencies (source or user) that fail to comply with the applicable restrictions and limitations of the NYSIC's privacy policy.

N. Training

1. The following individuals will participate in training programs regarding implementation of and adherence to this privacy, civil rights, and civil liberties policy:
   - All assigned personnel of the NYSIC;
   - Personnel providing information technology services to the NYSIC;
   - Staff in other public agencies or private contractors, as appropriate, providing tips, leads, and other data, SAR and ISE-SAR information technology or related services to the NYSIC;
   - User agency personnel and individuals authorized to access ISE-SAR information who are not employed by the NYSIC or a contractor.

2. The NYSIC's privacy policy training program will cover:
   - Purposes of the EE Initiative Privacy Policy;
   - Substance and intent of the provisions of the Policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of SAR and ISE-SAR information maintained or submitted by the NYSIC to the shared space;
   - How to implement the Policy in the day-to-day work of a participating agency;
   - The impact of improper activities associated with violations of the Policy;
   - Mechanisms for reporting violations of the Policy; and
   - The possible penalties for policy violations, including transfer, dismissal, and criminal liability, if any.

SAR Privacy Policy - Terms and Definitions
[SAR Appendix A]

The following is a list of primary terms and definitions used throughout this policy document.

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.

Acquisition—refers to 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 either 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—Agency refers to the NYSIC and all agencies that access, contribute, and share information in the NYSIC's justice information system.

Audit Trail—Audit trail is a generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail—what commands were issued to the system, what records and files were accessed or modified, etc.

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

Center—Center refers to the New York State Intelligence Center (NYSIC).

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

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

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

Data—Elements 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.

Fusion Center— A collaborative effort of two or more agencies that provide resources, expertise, and information to a designated government agency or agency component with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity.

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.

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

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

ISE-SAR—A suspicious activity report (SAR) that has been determined, pursuant to a two-part process, to have a potential terrorism nexus. ISE-SAR business rules will serve as a unifying process to support the reporting, tracking, processing, storage, and retrieval of terrorism-related suspicious activity reports across the ISE.

ISE-SAR Information Exchange Package Documentation (IEPD) —A schema that facilitates the posting and sharing of ISE-SAR information. The ISE-SAR IEPD is used to represent ISE information in two different data formats:

(1) The **Detailed format** includes information contained in all data elements set forth in Section IV of the ISE-SAR FS ("ISE-SAR Exchange Data Model"), including fields denoted as privacy fields.

(2) The **Summary format** excludes certain privacy fields as identified in the ISE-SAR FS. The ISE-SAR FS identifies the minimum privacy fields that must be excluded. Each ISE participant may exclude additional privacy fields from its Summary ISE-SARs, in accordance with applicable legal requirements.

Law—As used by this policy, law includes any local, state, or federal 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.

Logs—See Audit Trail. Logs are a necessary part of an adequate security system because they are needed to ensure that data is properly tracked and that only authorized individuals are getting access to the system and the data.

Participating Agencies—Participating agencies, for purposes of the EE Initiative, include source [the agency or entity that originates SAR (and, when authorized, ISE-SAR) information], submitting (which is the agency or entity posting ISE-SAR information to the shared space), and user (which is an agency or entity authorized by the submitting agency or other authorized agency or entity, to access ISE-SAR information, including information in the shared space(s), and which may include analytical or operational component(s) of the submitting or authorizing agency or entity) agencies, in support of their responsibility to collect, document, process, access, or use SAR and ISE-SAR information.

Personal Information— Information which can be used, either alone or in combination with other information, to identify individual subjects suspected of engaging in an activity or incident potentially related to terrorism.

Privacy—Privacy refers to individuals' interests in preventing the inappropriate collection, use, and release of personal information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. Other definitions of privacy include the right 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 Fields—Data fields in ISE-SAR IEPD's that contain personal information.

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

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

Protected Information—For the non-intelligence community, protected information is information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and laws of the United States. For state, local, and tribal governments, the protections derived from applicable state and tribal constitutions and state, local, and tribal laws, ordinances, and codes. For the (federal) intelligence community, protected information includes information about "United States persons" as defined in Executive Order 12333. Protected information may also include other information that the U.S. government expressly determines by Executive Order, international agreement, or other similar instrument should be covered.

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 agency's/center's information;
- Media organizations; and
- Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the agency.

Public does not include:

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

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.

Retention—Refer to Storage.

Role-Based Access—A type of access that uses roles to determine rights and privileges. A role is a symbolic category of users that share the same security privilege.

Security—Security refers to the range of administrative, technical, and physical business practices and mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes. Computer and communications security efforts also have the goal of ensuring the accuracy and timely availability of data for the legitimate user set, as well as promoting failure resistance in the electronic systems overall.

Shared Space—A networked data and information repository that is under the control of submitting agencies and which provides terrorism-related information, applications, and services to other ISE participants.

Sharing—Refers to the act of one ISE participant disseminating or giving homeland security information, terrorism information, or law enforcement information to another ISE participant.

Source Agency—Source agency refers to the agency or entity that originates 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:

1. Storage is frequently used to mean the devices and data connected to the computer through input/output operations—that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-computer storage. This meaning is probably more common in the IT industry than meaning 2.
2. 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, to include homeland security information, terrorism information, and law enforcement information relating to terrorism or the security of our homeland by both the originator of the information and any recipient of the information.

Submitting Agency—Submitting agency refers to the agency or entity providing ISE-SAR information to the shared space)

Suspicious Activity—Suspicious activity is defined as "reported or observed activity and/or behavior that, based on an officer's training and experience, is believed to be indicative of intelligence gathering or preoperational planning related

to terrorism, criminal, or other illicit (illegal) intention." Examples of suspicious activity include surveillance, photography of facilities, site breach or physical intrusion, cyber attacks, testing of security, etc.

Suspicious Activity Reports (SARs)—Record the observation and documentation of a suspicious activity. Suspicious activity reports (SARs) are meant to offer a standardized means for feeding information repositories. Any patterns identified during SAR review and analysis may be investigated in coordination with the reporting agency and, if applicable, the state-designated fusion center. Suspicious activity reports are not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor are they designed to support interagency calls for service.

Terrorism Information—Consistent with Section 1016(a)(4) of 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 IRTPA, as recently amended by the 9/11 Commission Act enacted on August 3, 2007 (P.L. 110-53), the ISE facilitates the sharing of terrorism and homeland security information, as defined in IRTPA Section 1016(a)(5) and the Homeland Security Act 892(f)(1) (6 U.S.C. § 482(f)(1)). See also Information Sharing Environment Implementation Plan (November 2006) and Presidential Guidelines 2 and 3 (the ISE will facilitate the sharing of "terrorism information," as defined in IRTPA, as well as the following categories of information to the extent that they do not otherwise constitute "terrorism information:" (1) homeland security information as defined in Section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. § 482(f)(1)); and (2) law enforcement information relating to terrorism or the security of our homeland). Such additional information includes intelligence information.

Weapons of Mass Destruction (WMD) information as a fourth (third statutory) category of ISE information is not called for in P.L. 110-53. Rather, it amends the definition of terrorism information to include WMD information and then defines that term. WMD information probably should not technically be cited or referenced as a fourth category of information in the ISE.

Tips and Leads Information or Data—Uncorroborated report or information generated from inside or outside the agency that alleges or indicates some form of possible criminal activity. Tips and leads can also be referred to as suspicious incident reports (SIRs), suspicious activity reports (SARs), and/or field interview reports (FIRs). Tips and leads information does not include incidents that do not have an offense attached, criminal history records, or Computer Aided Dispatch (CAD) data.

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 has some suspicion or mere suspicion attached to it, but without further inquiry or analysis, it is unknown whether the information is accurate or useful. Tips and leads information falls between being of no use to law enforcement and being extremely valuable depending on whether time and resources are available to determine its meaning.

Tips and leads information is maintained in a secure system, similar to data that rises to the level of reasonable suspicion.

User Agency—User agency refers to the agency or entity authorized by the submitting agency, or other authorized agency or entity, to access ISE-SAR information in the shared space(s), and which may include analytical or operational component(s) of the submitting or authorizing agency or entity.

Appendix D – Confidentiality and Nondisclosure Agreement

New York State Intelligence Center (NYSIC)
Confidentiality and Non-Disclosure Agreement (CNDA)

This constitutes an Agreement by and between the New York State Intelligence Center (NYSIC) and _____. By signing this CNDA, I accept that in order to be granted access to "sensitive information," I agree that I will keep such information confidential. "Sensitive information" includes:

a. **Law Enforcement Sensitive (LES)**: information that could adversely affect ongoing investigations, create safety hazards for officers, divulge sources of information, reveal tactics and strategies, and/or compromise identities.

b. **For Official Use Only (FOUO)**: information which warrants a degree of protection and administrative control that meets the criteria for exemption from public disclosure under the Privacy Act, and state and federal Freedom of Information Acts.

"Information" includes, but is not limited to: reports, files, folders, memoranda, statements, examinations, transcripts, images, and communications (eg meetings, briefings, and conversations).

1. Systems will be accessed only for legitimate governmental purposes. Information obtained in relation to reviewing and producing intelligence shall be limited to purposes directly connected with the duties and responsibilities of my assigned position.
2. I agree to keep confidential all sensitive information provided by the NYSIC and its participating agencies and to protect confidentiality and restrict access based on a right and need to know. Sensitive information disseminated by the NYSIC shall not be further disseminated without supervisory approval.
3. I understand that the unauthorized disclosure of information could cause damage or irreparable injury to future or ongoing investigations and operations. I understand that I am obligated to comply with the NYSIC's standard operating procedures regarding the authorized disclosure of such information.
4. Any compromise or suspected compromise of this Agreement must be reported to the appropriate supervisor and to the NYSIC Security Officer. I understand the New York State Police may seek any remedy available to enforce this Agreement and to protect the security of its information assets. Non-compliance with this policy that results in the compromise of information confidentiality, integrity and/or availability can result in administrative disciplinary action, and/or possible criminal prosecution under applicable local, state, and federal laws.
5. I understand that by signing this Agreement, all sensitive information to which I have access or may obtain access is and will remain the property of the NYSIC. In addition, I hereby assign to the New York State Police all royalties, remunerations, and emoluments that have resulted or may result from any disclosure, publication, or revelation of "sensitive information" not consistent with the terms of this Agreement.
6. I agree that exceptions to this CNDA policy will be documented in writing and submitted for approval to the Director of the NYSIC or the NYSIC Security Officer. If approved, the exception will be kept on file.
7. I hereby acknowledge that I have read this Agreement in full concerning the nature and protection of sensitive information. This agreement shall be kept on file with the NYSIC.

_____	_____
Print Name and Org./Agency	Print Security Officer's Name and Agency
_____	_____
Signature Date	Security Officer's Signature Date