NEW JERSEY ROIC PRIVACY POLICY

MISSION STATEMENT

The mission of the New Jersey Regional Operations Intelligence Center (NJROIC) is to interface with the New Jersey law enforcement community, and other law enforcement and homeland security agencies, by being a primary point of contact for collection, evaluation, analysis, and dissemination of intelligence data and criminal background information in a timely and effective manner in order to detect and/or prevent criminal or terrorist activity, and to solve crimes. This mission shall remain consistent with the National Criminal Intelligence Sharing Plan. The purpose (goal) of the NJROIC Privacy Policy is to ensure protection of the privacy, civil rights, and civil liberties of individuals and organizations.

The goal of establishing and maintaining the NJROIC is to further the following purposes:

- Be an active participant in the Information Sharing Environment.
- Increase public safety and security in the State of New Jersey, the region and to contribute to the security of the nation.
- Mitigate or minimize the threat and risk of injury to all members of the public safety and health care communities.
- Mitigate or minimize the threat and risk of damage to real or personal property.
- Protect the individual privacy rights, civil rights or other protected interests a person or persons may have.
- Protect the integrity of the criminal investigative, criminal intelligence, and justice system processes and information.

- Foster relationships with persons or groups of people in an effort to promote cooperation between law enforcement and the community which it serves.

- Make the most effective use of public safety resources.

The NJROIC is not an independent, operational investigative entity.

POLICY APPLICABILITY AND LEGAL COMPLIANCE

The NJROIC personnel, including enlisted personnel, sworn participating agency personnel, civilian New Jersey State Police (NJSP), participating agency personnel, private contractors, and civilian personnel providing information technology services to the NJROIC will comply with the privacy policy of the NJROIC. This policy shall apply to any information that the NJROIC collects, receives, maintains, archives, accesses, or discloses among its personnel, other government agencies (including Regional Intelligence Sharing Systems [RISS] and Information Sharing Environment [ISE] agencies), and partner criminal justice and public safety agencies, as well as quasi-government entities, private contractors, and the general public.

The NJROIC will provide a printed copy of this policy to all enlisted, civilian and partner agency personnel, as well as contractors who provide services and will require both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and all the provisions contained herein.

All New Jersey Regional Operations and Intelligence Center (NJROIC) personnel, sworn participating agency personnel, civilian and participating agency

personnel who provide information technology services to the NJROIC, the New Jersey State Police or any participating agency, private contractors and other authorized partners or users will comply with all applicable State and federal laws concerning the protection of privacy, civil rights, and civil liberties. See Appendix B for a list of applicable law.

The NJROIC has adopted internal operating policies that are in compliance with applicable laws protecting privacy, civil rights, and civil liberties, including applicable state and federal privacy, civil rights, and civil liberties law as set forth in Appendix B of this policy.

As it relates to the day-to-day operations of the NJROIC, this policy takes notice of the fact that operations at the NJROIC do not, in most cases, lead to the development of any new databases. The NJROIC personnel predominantly use existing databases that are, have been, and will continue to be, governed by their own statutory or regulatory language. Examples of such databases are the Criminal Justice Information System (CJIS), the Statewide Intelligence Management System (SIMS), and the Motor Vehicle Commission's (MVC) drivers' registry. It is the policy of the NJROIC to ensure that any rule, regulation, guideline, or mandate, with regard to the use or dissemination of any information or intelligence, is strictly adhered to by all personnel assigned to the NJROIC. It is not the intention of the NJROIC administrators to create rules or regulations that exceed any pre-existing rules or regulations, but to expect compliance with those standards already in place. As the NJROIC is an entity within the New Jersey State Police, a Division within the Department of Law and Public

Safety, all applicable policies of the Department will be adhered to by the NJROIC. Violations of this Privacy Policy by employees of the NJSP, enlisted and civilian, shall be disciplined in accordance with administrative procedures available to the Superintendent of the State Police. Outside agency personnel assigned to the NJROIC are subject to removal from assignment to the NJROIC by the Task Force Commander and shall be referred to their host agency for appropriate action. Participating agencies and individual users are subject to the enforcement procedures and sanctions provided in **Accountability and Enforcement**.

GOVERNANCE AND OVERSIGHT

Primary responsibility for the operation of the NJROIC, its justice systems, operations, coordination of personnel; the receiving, seeking retention, evaluation information quality, analysis, destruction, sharing or disclosure of information; and the enforcement of this policy is assigned to the Task Force Commander of the NJROIC.

The NJROIC is guided by a center-designated and trained Privacy Officer who liaises with community privacy advocacy groups to ensure that privacy, civil rights, and civil liberties are protected within the provisions of this policy and within the center's information, collection, retention and dissemination processes, and procedures. The Operations Officer is designated as the Privacy Officer.

The NJROIC has a Privacy Committee comprised of the Operations Officer, the Security Officer, and the Assistant Unit Heads for Watch Operations, Analysis Element, and Strategic Outreach. The Privacy Committee will annually review and recommend privacy policy updates to the Task Force Commander in response to changes in law

and implementation experience, including the results of audits and inspections. The NJROIC Privacy Committee is guided by the Privacy Officer who shall receive reports regarding alleged errors and violations of the provisions of this policy, receive and coordinate complaint resolution under the center's redress policy, serve as the liaison for the Information Sharing Environment (ISE), and ensure that privacy protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy-enhancing technologies. The Privacy Officer shall be thoroughly familiar with the Privacy Guidelines for the ISE. The Privacy Officer shall receive training from the Department of Law and Public Safety and/or the Division of State Police, where available. The Privacy Officer can be contacted at the following address: ROIC Privacy Office, 2 Schwarzkopf Drive, West Trenton, NJ 08628.

DEFINITIONS

Primary terms and definitions used in this policy are provided in Appendix A, Terms and Definitions

INFORMATION

The role of the NJROIC is linked closely with the Intelligence-Led Policing (ILP) initiative undertaken by the New Jersey State Police. Specifically, ILP is a collaborative philosophy based on improved intelligence operations to aid in understanding the changes in the operating environment to enable law enforcement to rapidly adjust to new circumstances.[1] In its most efficient state, ILP requires police officers and

[1] New Jersey State Police Practical Guide to Intelligence-Led Policing, Sept., 2006 , pg. 5

investigators to become better data collectors and better consumers of intelligence related products.[2]

The NJROIC will seek and retain information and/or intelligence that:

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

The above-described information may be stored in official State Police databases, Records Management Systems (RMS), intelligence management systems, or information/intelligence from other law enforcement entities with which the ROIC or the NJSP may have existing law enforcement relationships. Information may also be sought from available public sources.

It is acknowledged that some information or data collected by the NJROIC may be related to other domains, such as the Homeland Security function of collecting

[2] Ibid. pg. 6

information related to natural or man-made disasters, critical infrastructure, and health crises. This type of information does not associate people with criminal activity and therefore precluded from the requirement adherence to the information guidelines set forth this policy and the requirements applicable in 28 C.F.R. Part 23 and the Attorney General Guidelines on the Collection, Handling and Dissemination of Intelligence in New Jersey.

The NJROIC will not seek or retain, and information originating agencies will agree not to submit, information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular non-criminal organization or lawful event; or their race, ethnicity, citizenship, place or origin, age, disability, gender, or sexual orientation.

The NJROIC applies labels to center-owned information (and ensures that the originating agency has applied labels) to indicate to the accessing authorized user that: (1) The information contains personal data that is protected information (See Appendix A); and (2) the information is subject to State and Federal laws restricting access use or disclosure.

The NJROIC personnel will, upon receipt of information, assess the information to determine its nature and purpose. Personnel will assign information to categories to Indicate the result of the assessment, such as:

- Whether the information is general data, tips and leads data, suspicious activity reports, or criminal intelligence data;

- The nature of the source (i.e., anonymous tip, interview, public records, private sector);
- The reliability of the source (i.e., reliable, usually reliable, unreliable, unknown); and
- The validity of the content (i.e., confirmed, probable, doubtful, cannot be judged).

At the time a decision is made to retain information, it will be labeled pursuant to applicable limitations on access and sensitivity of disclosure in order to:

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

The labels assigned to 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.

The NJROIC will identify and review protected information that may be accessed from or disseminated by the center prior to sharing that information through the Information Sharing Environment. Further, the center will provide notice mechanisms, including but not limited to metadata or data field labels that will enable ISE authorized

users to determine the nature of the protected information and how to handle the information in accordance with applicable legal requirements.

The NJROIC requires certain descriptive information to be entered and electronically associated with each piece of data that is to be accessed, used, or disclosed, including terrorism-related information shared through the ISE, such as:

- The name of the originating department or entity;
- The name of the agency system from which the information is disseminated;
- The date the information was collected and the date its accuracy was last verified;
- The title and contact information for the persons or persons to who questions regarding the information can be directed.

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

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

TIPS AND LEADS AND SUSPICIOUS ACTIVITY REPORTS (SARs)

The NJROIC will also retain and share suspect information that does not reach the level of reasonable suspicion such as tips and leads or suspicious activity reports (SAR). In most privacy policies, it is widely accepted that information should be evaluated prior to any dissemination or sharing. While this principal is generally

accepted by the NJROIC as well, current protocols require Tips and Leads and SAR information to be transmitted immediately to the New Jersey Office of Homeland Security and Preparedness (OHS&P), county counter-terrorism coordinators and the local field office of the Federal Bureau of Investigation.

Specifically, NJROIC personnel are required to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention and security of Tips and Leads and SAR information:

NJROIC personnel will immediately transmit such information to the CTWATCH desk which is managed and maintained for the NJROIC by our partner agency, the OHS&P. It is acknowledged and understood that the New Jersey State Police, in compliance with New Jersey Attorney General's Memorandum of Understanding with the FBI-Newark and the FBI-Philadelphia, has agreed to transmit Tips and Leads and SARs to the FBI-JTTF and that OHS&P's CTWATCH has a procedure in place to immediately forward Tips and Leads and SARs to the FBI for review. This forwarding of information is done prior to any attempt to validate or refute the information.

In the event such information is to be returned to the NJROIC by the FBI or OHS&P, prior to further access to or dissemination of the information, OHS&P personnel will, pursuant to a Memorandum of Agreement with the NJROIC:

- Attempt to validate or refute the information and assess it for sensitivity and confidence;
- Subject the information to an evaluation process to determine its credibility and value and to categorize the information as unsubstantiated or uncorroborated after attempts to validate the information fail;

- 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 access or dissemination method that is used for data that rises to the level of reasonable suspicion, (i.e., right-to-know, need-to-know).

- Regularly provide access to or disseminate the information in response to an interagency inquiry for law enforcement, homeland security, or public safety and analytical purposes, or when credible information indicates a potential imminent danger to life or property.

- Retain information for up to one year to work a tip or lead to determine its credibility and value, assign a "disposition" label (i.e. unresolved, cleared, unfounded, forwarded to SIMS) so that an authorized user knows that status and purpose for the retention and will retain the information based upon the retention period associated with the disposition label.

- Adhere to and follow the NJROICs physical, administrative, and technical security measures that are in place for the protection and security of tips and leads and SARs. Tips and Leads and SARs will be secured in a manner consistent with SIMS data.

Tip and Lead and SAR information will he processed, stored, and disseminated by OHS&P on behalf of NJROIC under a Memorandum of agreement between the agencies the requires a separate policy SAR policy that is appended as Appendix C to this policy.

ACQUIRING AND RECEIVING INFORMATION

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

- 28 CFR Part 23 regarding criminal intelligence information.
- The OECD Fair Information Principles (under certain circumstances, there may be exceptions to the Fair Information Principles, based, for example, on authorities paralleling those provided in the federal Privacy Act; state, local, and tribal law; or center policy).

- Criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) *National Criminal Intelligence Sharing Plan* (NCISP).
- Constitutional provisions; New Jersey statutes; Attorney General Guidelines; and administrative rules, as well as regulations and policies that apply to multijurisdictional criminal intelligence information databases. See Appendix B for a list of specific law applicable to NJROIC operations.

Information-gathering and investigative techniques used by the NJROIC will, and those used by originating agencies should, be the least intrusive means necessary in the particular circumstances to gather information it is authorized to seek or retain.

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

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

The NJROIC will not directly or indirectly receive, seek, accept, or retain information from:

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

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

INFORMATION QUALITY ASSURANCE

The NJROIC will make all reasonable efforts to ensure that information sought or

retained is derived from dependable and trustworthy sources of information, collected in an authorized

and lawful manner; in compliance with the Attorney General Guidelines on

the Collection, Handling, Storage, and Dissemination of Intelligence in New Jersey,

and is accurate, current, and complete, and merged with other information about the same individual or organization when applicable standards (See **Merger**) have been met.

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

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

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

The NJROIC will conduct periodic data quality reviews of information it originates and make every reasonable effort to ensure that the information will be corrected, deleted from the system, or not used when the center identifies information that is erroneous, misleading, obsolete, or otherwise unreliable; the center did not have authority to gather the information or to provide the information to another agency; or the center used prohibited means to gather the information (except when the center's information source did not act as the agent of the center in gathering the information).

Originating agencies external to the NJROIC are responsible for reviewing the quality and accuracy of the data provided to the center. The center will review the quality of information it has received from an originating agency and advise the appropriate contact person in the originating agency, in writing or electronically, if its data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable.

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

COLLATION AND ANALYSIS

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

Information subject to collation and analysis is information as defined and identified in **INFORMATION**.

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

- Further crime prevention (including terrorism), law enforcement, public safety, force deployment, or prosecution objectives and priorities established by the center.
- Provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal (including terrorist) activities.

MERGING RECORDS

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

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

SHARING AND DISCLOSURE

Credentialed, role-based access criteria will be used by the NJROIC, as appropriate, to control:

- The information to which a particular group or class of users can have access based on the group or class.
- The information a class of users can add, change, delete, or print.
- To whom, individually, the information can be disclosed and under what circumstances.

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

Agencies external to the NJROIC may not disseminate information accessed or disseminated from the center without approval from the center or other originator of the information.

Records retained by the NJROIC may be accessed by or disseminated ***to those responsible for public protection, public safety, or public health*** only for public protection, public safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures. An audit trail sufficient to allow the identification of each individual who accessed or received information

retained by the center and the nature of the information accessed will be kept by the center.

Information gathered or collected and records retained by the NJROIC may be accessed or disseminated ***for specific purposes*** upon request by persons authorized by law to have such access and only for those uses and purposes specified in the law. An audit trail sufficient to allow the identification of each individual who requested, accessed, or received information retained by the center; the nature of the information requested, accessed, or received; and the specific purpose will be kept for a minimum of five (5) years by the center.

Information gathered or collected and records retained by the NJROIC may be accessed or disclosed ***to a member of the public*** only if the information is defined by law to be a public record or otherwise appropriate for release to further the center's mission and is not exempt from disclosure by law. Such information may be disclosed only in accordance with the law and procedures applicable to the center for this type of information. An audit trail sufficient to allow the identification of each individual member of the public who accessed or received information retained by the center and the nature of the information accessed will be kept by the center.

Information gathered or collected and records retained by the NJROIC ***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 disclosure or publication, unless disclosure is agreed to as part of the normal operations of the agency.
- Disseminated to persons not authorized to access or use the information.

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

- Records required to be kept confidential by law are exempted from disclosure requirements under the Open Public Records Act, P.O. 2001, Chapter 404 N.J.S. 47;1A-3, Executive Order #26, Executive Order #9 (Hughes 1963), and as affirmed by the Government Records Council final decision # 2002-30 dated February 13th 2003.
- Information that meets the definition of "classified information" as that term is defined in the National Security Act, Public Law 235, and Section 606.
- Investigatory records of law enforcement agencies that are exempted from disclosure requirements under [the Open Public Records Act, P.O. 2001, Chapter 404 N.J.S. 47;1A-3, Executive Order #26, Executive Order #9 (Hughes 1963), and as affirmed by the Government Records Council final decision # 2002-30 dated February 13th 2003. However, certain law enforcement records must be made available for inspection and copying under the stated regulations.
- A record or part of a record the public disclosure of which would have a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack is exempted from disclosure requirements under the Open Public Records Act, P.O. 2001, Chapter 404 N.J.S. 47; 1A-3, Executive Order #26, Executive Order #9 (Hughes 1963), and as affirmed by the Government Records Council final decision # 2002-30 dated February 13th 2003. This includes a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism or an act of agricultural terrorism, vulnerability assessments, risk planning documents, needs assessments, and threat assessments.
- Protected federal, state, local, or tribal records, which may include records originated and controlled by another agency that cannot, under 28 C.F.R part 23, the Open Public Records Act, P.O. 2001, Chapter 404 N.J.S. 47; 1A-3, Executive Order #26, Executive Order #9 (Hughes 1963), and as affirmed by the Government Records Council final decision # 2002-30 dated February 13th 2003, and the New Jersey Attorney Generals guidelines, be shared without permission.
- A violation of an authorized nondisclosure agreement under the Attorney Generals Guidelines the Open Public Records Act, P.O. 2001, Chapter 404 N.J.S. 47;1A-3, Executive Order #26, Executive Order #9 (Hughes 1963), and as affirmed by the Government Records Council final decision # 2002-30 dated February 13th 2003.

The NJROIC will not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information unless otherwise required by law.

REDRESS

In instances where a member of the public seeks to obtain information within the databases of the NJROIC, such requests shall be directed to the Department of Law and Public Safety and in compliance with the provisions of the New Jersey Open Public Records Act (P.L. 2001, c. 404, N.J.S. 47:1A-1 et seq.**).** Where the Department declines such requests, any appeals of the request must be made to the Department.

A record will be kept of all requests for NJROIC information and of what information is disclosed to an individual.

The existence, content, and source of the information will not be made available by the Department of Public Safety to an individual when the information is exempt from disclosure under the NJ Open Public Records Act - P.L. 2001, CHAPTER 404, N.J.S. 47:1A-1 et seq. or other applicable law.

If the information does not originate with the center, the requestor will be referred by the Department of Law and Public Safety to the originating agency, if appropriate or required by law, or the source agency will be notified of the request and the determination that disclosure by the Department of Law and Public Safety or referral of the requestor to the source agency was neither required nor appropriate under applicable law.

If an individual requests correction of information originating with the NJROIC that has been disclosed, the Department of Law and Public Safety will inform the individual of the procedure for requesting and considering requested corrections, including appeal rights if requests are denied in whole or in part. A record will be kept of all requests for corrections and the resulting action, if any.

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

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

(a) Is exempt from disclosure,

(b) Has been or may be shared through the ISE,

(1) Is held by the NJROIC and

(2) Allegedly has resulted in demonstrable harm to the complainant,

The center will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the center's Privacy Officer at the following address: NJ Regional Operations Intelligence Center, 2 Schwarzkopf Drive, West Trenton, New Jersey 08628. The Privacy Officer will

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

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

SECURITY

Information stored in electronic data systems in the NJROIC are governed and regulated by the Section Data Manager of the Division of State Police (DSP), who shall serve as the trained Security Officer for the center.

The ROIC is a secure facility whose access is controlled by a magnetic swipe card system to prevent external intrusion. Access cards are available only to personnel who meet the requirements as stated in the Security Protocols promulgated by the Director. Only individuals who work in the Analysis Element will be allowed into that area of the building. The center will utilize secure internal and external safeguards against network intrusions. The ROIC utilizes a two-factor authentication verification for external safeguards to guard against unauthorized network intrusions. Access to the center's databases from outside the facility is only available by Virtual Private Network through a Secured Socket Layer Certificate server.

Outside partner agencies assigned to the NJROIC may have independent computer systems controlled by that agency. Examples of such instances are the United States Department of Homeland Security, and the Federal Bureau of Investigation. These agencies are responsible for clearance and access to their databases in accordance with their own security procedures.

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

Access to NJROIC information will be granted only to center and Division of State Police personnel whose positions and job duties require such access; who have successfully completed a background check and appropriate security clearance, if applicable; and who have been selected, approved, and trained accordingly.

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

The NJROIC will utilize watch logs to maintain audit trails of requested and disseminated information.

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

The NJROIC will follow the data breach notification law set forth in N.J. Stat. 56:8-163.

INFORMATION RETENTION AND DESTRUCTION

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

When information has no further value or meets the criteria for removal according to the NJROIC's retention and destruction policy or according to applicable law (28 CFR Part 23), it will be purged, destroyed, and deleted or returned to the submitting (originating) agency.

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

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

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

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

ACCOUNTABILITY AND ENFORCEMENT

The NJROIC will be open with the public in regard to information and intelligence collection practices. The center's privacy policy will be made available upon request and posted on the Division of State Police Web site (http://www.njsp.org/).

The NJROIC's Privacy Officer will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s) maintained or accessed by the center. The Privacy Officer can be contacted at NJ Regional Operations Intelligence Center, 2 Schwarzkopf Drive, West Trenton, New Jersey 08628.

The audit log of queries made to the NJROIC will identify the user initiating the query. The center will maintain an audit trail of accessed, requested, or disseminated information. An audit trail will be kept for a minimum of 5 (five) years of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.

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

The ROIC's personnel and other authorized users shall report errors and suspected or confirmed violations of center policies relating to protected information to the center's Privacy Officer. (See **GOVERNANCE AND OVERSIGHT**).

The NJROIC will annually conduct an audit and inspection of the information and intelligence contained in its information system(s). The audit will be conducted by the center's Privacy Officer. This Privacy Officer has the option of conducting a random audit, without announcement, at any time and without prior notice to staff of the center. The audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of

the center's information and intelligence system(s).

The NJROIC's Privacy Committee will review and recommend updates of the provisions protecting privacy, civil rights, and civil liberties contained in this policy annually in response to changes in applicable law, technology, the purpose and use of the center's information systems, and public expectations.

Violations of this Privacy Policy by employees of the NJSP, enlisted and civilian, shall be disciplined in accordance with administrative procedures available to the Superintendent of the State Police. Outside agency personnel assigned to the NJROIC

are subject to removal from assignment to the NJ ROIC by the Director and shall be referred to their host agency for appropriate action.

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

TRAINING

All persons assigned to the NJROIC, at a minimum, will receive annual Privacy training in accordance with the standards of the NJSP Training Academy. In addition, the center will require the following individuals to participate in training programs regarding implementation of and adherence to the privacy, civil rights, and civil liberties policy:

- Personnel providing information technology services to the center.
- Staff in other public agencies or private contractors providing services to the center.
- Users who are not employed by the center or a contractor.

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

The NJROIC's privacy policy training program will cover:

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

- Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the center.
- Originating and participating agency responsibilities and obligations under applicable law and policy.
- How to implement the policy in the day-to-day work of the user, whether a paper or systems user.
- The impact of improper activities associated with infractions within or through the agency.
- Mechanisms for reporting violations of center privacy protection policies and procedures.
- The nature and possible penalties for policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.

APPENDIX A –Terms and Definitions

Access—Data access is being able to get to (usually having permission to use) particular data on a computer. Web access means having a connection to the World Wide Web through an access provider or an online service provider. Data access is usually specified as read-only and read/write access.

With regard to the ISE, access refers to the business rules, means, and processes by and through which ISE participants obtain terrorism-related information, to include homeland security information, terrorism information, and law enforcement information acquired in the first instance by another ISE participant.

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

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

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

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

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

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

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.40 Fusion Center Privacy Policy Development

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

Center—Refers to the NJ ROIC and all participating state agencies of the NJ ROIC.

Civil Liberties—Fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights—the first ten Amendments to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference. Generally, the term “civil rights” involves positive (or affirmative) government action, while the term “civil liberties” involves restrictions on government.

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

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

Confidentiality—Closely related to privacy but is not identical. It refers to the obligations of individuals and institutions to use information under their control appropriately once it has been disclosed to them. One observes rules of confidentiality out of respect for and to protect and preserve the privacy of others. 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 Information—Information deemed relevant to the identification of and the criminal activity engaged in by an individual who or organization that is reasonably suspected of involvement in criminal activity. Criminal intelligence records are maintained in a criminal intelligence system per 28 CFR Part 23.

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

Data Breach—The unintentional release of secure information to an untrusted environment. This may include incidents such as theft or loss of digital media—including computer tapes, hard drives, or laptop computers containing such media—upon which such information is stored unencrypted; posting such information on the World Wide Web or on a computer otherwise accessible from the Internet without proper information security precautions; transfer of such information to a system that is not completely open but is not appropriately or formally accredited for security at the approved level, such as unencrypted e-mail; or transfer of such information to the information systems of a possibly hostile agency or environment where it may be exposed to more intensive decryption techniques.

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

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

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

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

Fair Information Principles—The Fair Information Principles (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:

- Collection Limitation Principle
- Data Quality Principle
- Purpose Specification Principle
- Use Limitation Principle

Security Safeguards Principle•
Openness Principle•
Individual Participation Principle•
Accountability Principle•

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

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

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

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

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

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

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

conventional views of the topic to include considerations of accessibility, security, and privacy.

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

Intelligence-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.

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

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

Law Enforcement Information—For purposes of the ISE, law enforcement information means any information obtained by or of interest to a law enforcement agency or official that is both (a) related to terrorism or the security of our homeland and (b) relevant to a law enforcement mission, including but not limited to information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of or response to criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of or response to criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance.

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

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

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

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

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

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

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

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

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

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

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

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

Personal characteristics (such as height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation, place of birth, mother's maiden name, distinguishing features, and biometrics information, such as fingerprints, DNA, and retinal scans).

A unique set of numbers or characters assigned to a specific individual (including name, address, phone number, social security number, e-mail address, driver's license number, financial account or credit card number and associated PIN number, Integrated Automated Fingerprint Identification System [IAFIS] identifier, or booking or detention system number). Descriptions of event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records).

Descriptions of location(s) or place(s) (including geographic information systems [GIS] locations, electronic bracelet monitoring information, etc.).

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

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

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

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

Protected Information—Information about individuals that is subject to information privacy or other legal protections under the Constitution and laws of the United States and the State of New Jersey. Protection may be extended to organizations by federal regulation (28 CFR Part 23) or State policy.

Public—Public includes:

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

Public does not include:

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

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

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

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

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

Retention—Refer to Storage.

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

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

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

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

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

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

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

In a more formal usage, storage has been divided into (1) primary storage, which holds data in memory (sometimes called random access memory, or RAM) and other "built-in" devices such as the processor's L1 cache, and (2) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations.

Primary storage is much faster to access than secondary storage because of the proximity of the storage to the processor or because of the nature of the storage devices. On the other hand, secondary storage can hold much more data than primary storage.

With regard to the ISE, storage (or retention) refers to the storage and safeguarding of terrorism-related information—including homeland security information, terrorism information, and law enforcement information relating to terrorism or the security of our homeland—by both the originator of the information and any recipient of the information.

Suspicious Activity—Defined in the ISE-SAR Functional Standard (Version 1.5) as "observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity." Examples of suspicious activity include surveillance, photography of sensitive infrastructure facilities, site breach or physical intrusion, 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 the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended by the 9/11 Commission Act (August 3, 2007, P.L. 110-53), the ISE facilitates the sharing of terrorism and homeland security information, as defined in IRTPA Section 1016(a)(5) and the Homeland Security Act 892(f)(1) (6 U.S.C. § 482(f)(1)). See also *Information Sharing Environment Implementation Plan* (November 2006) and Presidential Guidelines 2 and 3 (the ISE will facilitate the sharing of "terrorism information," as defined in the IRTPA, as well as the following categories of information to the extent that they do not otherwise constitute "terrorism information": (1) homeland security information as defined in Section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. § 482(f)(1)); and (2) law enforcement information relating to terrorism or the security of our homeland). Such additional information may include intelligence information.

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

Tips and Leads Information or Data—Generally uncorroborated reports or information generated from inside or outside a law enforcement agency that allege or indicate some form of possible criminal activity. Tips and leads are sometimes referred to as suspicious incident report (SIR), suspicious activity report (SAR), and/or field interview report (FIR) information. However, SAR information should be viewed, at most, as a

subcategory of tip or lead data. Tips and leads information does not include incidents that do not have a criminal offense attached or indicated, criminal history records, or CAD data. Tips and leads information should be maintained in a secure system, similar to data that rises to the level of reasonable suspicion.

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

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

APPENDIX B -- Applicable Law

Applicable Statutes, Directives, Guidelines Used for Privacy Policy Legal Compliance

- Executive Order #5 (03-16-06)
- Attorney General Memo – Guidelines for Dissemination of the NJ Public and Law Enforcement (10-09-07)
- Attorney General Guidelines on Collection, Handling, Storage and Dissemination of Intelligence in NJ (03/09/05)
- Domestic Security Preparedness Task Force Act
- U.S. Constitution
- NJ Constitution
- NJ Open Public Records Act - P.L. 2001, CHAPTER 404, N.J.S. 47:1A-1 et seq.
- NJ Law Against Discrimination
- CJIS Policies
- Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) Privacy, Civil Rights, and Civil Liberties Protection Policy
- New Jersey Intelligence System Operating Policy and Procedures

New Jersey Office of Homeland Security and Preparedness and New Jersey Regional Operations Intelligence Center

Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) Privacy, Civil Rights, and Civil Liberties Protection Policy

A. Purpose Statement

1. The purpose of the Nationwide SAR Initiative (hereafter "NSI") Privacy, Civil Rights, and Civil Liberties Protection Policy (hereafter "Privacy and CR/CL Policy") is to promote the New Jersey Office of Homeland Security and Preparedness (OHSP) and the New Jersey Regional Operations Intelligence Center (NJROIC, hereafter "FC" or "submitting agency"), source agency, and user agency (hereafter collectively referred to as "participating agencies" or "participants") conduct under the NSI that complies with applicable federal, state, local, and tribal law, including constitutional law, statutes, regulations, executive orders, 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.

B. Policy Applicability and Legal Compliance

1. All participating FC personnel, including New Jersey Office of Homeland Security and Preparedness (OHSP) personnel providing SAR processing services[3], personnel providing SAR-related information technology services to the FC or OHSP, private contractors, and other authorized participants will comply with applicable provisions of the OHSP and FC's Privacy and CR/CL Policy concerning personal information, including:
   - SAR information a source agency gathers or collects and the OHSP/FC receives; *and*
   - The ISE-SAR information identified, submitted to a Shared Space, and accessed by or disclosed to OHSP/FC personnel or FC participants.

[3] OHSP will provide SAR processing services under an interagency agreement with the NJROIC. Hereafter, references to the NJROIC as the FC or submitting agency shall be deemed to include and be applicable to OHSP personnel and contactors providing SAR processing services on behalf of the NJROIC under this policy and in accordance with the referenced interagency agreement.

2. The OHSP and FC will provide a printed copy of its Privacy and CR/CL Policies to all FC personnel, nonagency personnel who provide services to the FC and to each source agency and FC authorized user 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 OHSP and FC personnel, participating agency personnel, personnel providing information technology services to the FC, private contractors, and other authorized users shall comply with applicable law 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 FC and/or other participating agencies (see Appendix C).

C. Governance and Oversight

1. The Director of the FC, in coordination with the Director of the OHSP, will have primary responsibility for: operating the FC, ISE-SAR information system operations, and coordinating personnel involved in the NSI; 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. Day to day supervision of the OHSP Counter Terrorism Watch (CTWatch) will be provided by OHSP. CTWatch is based at the FC.

2. The FC's participation in the NSI will be guided by a trained OHSP Privacy Officer who is appointed by the OHSP 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, receive and coordinate complaint resolution under the center's redress policy, and serve as the liaison for the Information Sharing Environment. The OHSP Privacy Officer can be contacted at the following address: Maureen Lancaster, Phone: 609-584-4349, Email: Maureen.lancaster@ohsp.state.nj.us

D. Terms and Definitions

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

E. Information

1. The FC, directed by the OHSP CTWatch, will seek or retain information that a source agency (the FC or other agency) 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 behavior; 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 source agency assures was acquired in accordance with agency policy and in a lawful manner.

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

3. Upon receipt of SAR information from a source agency that has processed the information in accordance with OHSP/FC criteria (business processes set forth in the NJ SARs Procedures Manual), designated CTWatch personnel will:
   - Personally review and vet the SAR information 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 shared space; and
   - Notify the source agency that the SAR has been identified as an ISE SAR and submitted to the shared space.

4. The CTWatch will ensure that certain basic and special descriptive information is entered and electronically associated with ISE-SAR information, including:
   - The name of the source agency;
   - 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 current version of the Information Sharing Environment (ISE) Functional Standard - Suspicious Activity Reporting (SAR) (SAR Functional Standard):
   - 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 levels, including:
     - Source Reliability Codes

     A. Completely Reliable – This code refers to a source about whom there is no doubt of its authenticity, trustworthiness, or competency. Information supplied by a person who in the past has proved to be reliable in all instances.

B. Mostly Reliable – This code refers to a source about whom or which there may be occasional doubt as to authenticity, trustworthiness, precision or to its competency. However, information obtained from the source in the past has, in the majority of instances, proved to be reliable.

C. Somewhat Reliable – This code refers to a source about whom there is usually some doubt as to authenticity and trustworthiness. Information obtained from this source in the past, has proved reliable in a moderate number of cases.

D. Unreliable – This code refers to a source about whom or which there is doubt as to its authenticity and trustworthiness. Information supplied by this source in the past has not proved to be reliable.

E. Reliability Unknown – This code refers to a source whose reliability has not been determined by either experience or investigation. There is no way of knowing the authenticity, trustworthiness, or competency of information supplied by this source. A newly-developed confidential informant falls into this category of source reliability.

- Information Reliability Codes
  1. Known to be True/Confirmed True – This information has been corroborated or is known by personal observation of the report creator to be absolutely true.

  2. Probably True - This information is consistent with past accounts provided by other sources regarding this topic.

  3. Possibly True – This information is not entirely consistent with past accounts, but is believed by the report creator to be plausible.

  4. Cannot be Judged – This information cannot be evaluated or judged.

  5. Identification Data – This information has been entered for identification purposes only and there is positively no inference of criminal activity intended or implied.

- Due diligence will be exercised in determining source reliability and content validity. Information determined not to meet NJSARS standards by the CTWatch Compliance Unit will not be retained in NJSARS. Additionally, information determined to be unfounded will be purged from the shared space.
- Unless otherwise indicated by the source or 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, OHSP CTWatch compliance staff will ensure that the ISE-SAR information is labeled, to the maximum extent feasible and consistent with the SAR Functional Standard, 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 OHSP CTWatch staff will share ISE-SAR information with authorized non-fusion center agencies and individuals only in accordance with established NJSAR and FC policy and procedure.

8. The OHSP CTWatch staff 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 OHSP/FC 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 source agencies must comply with and adhere to applicable law, 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 FCs and source agencies who acquire SAR information that may be shared with the FC will be trained to recognize behaviors that are 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 New Jersey Constitution, applicable federal and state law, NJSARS policies (as per Appendix B and C), and NSI Program Management Office policy guidance applicable to the NSI.

G. Information Quality Assurance

1. The OHSP CTWatch staff will ensure that source agencies assume primary responsibility for the quality and accuracy of the SAR data collected by the CTWatch. The CTWatch will advise the appropriate contact person in the source agency in writing (this would include electronic notification) if SAR information received from the source agency is alleged, suspected, or found to be erroneous or deficient.

2. The CTWatch staff will make every reasonable effort to ensure that SAR information collected and ISE-SAR information retained and posted to the shared space is derived from dependable and trustworthy source agencies and is as accurate, current, and complete as possible, including meeting standards set in the NJSARS Compliance Policy.

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).

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 quality or 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 the source agency did not have authority to acquire the original SAR information, used prohibited means to acquire it, did not have authority to provide it to the CTWatch, 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 CTWatch staff will provide written notice (this would include electronic notification) to the source agency that provided the SAR, 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 CTWatch is corrected or removed from the shared space by the OHSP/FC because it is erroneous or deficient such that the rights of an individual may be affected. A record of such changes must be kept on file as part of the automated notification system.

H. Analysis

1. ISE-SAR Information posted by the CTWatch staff to the shared space or accessed from the shared spaces under the NSI will be analyzed for intelligence purposes only by qualified OHSP/FC personnel or other qualified user agencies 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 OHSP/FC, 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. Only those members of the law enforcement or the intelligence community successfully completing the NJSARS training course will have access to NJSARS. 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 NSI Program Management Office, the OHSP/FC will adhere to the SAR Functional Standard for the ISE-SAR process, including the use of the ISE-SAR IEPD reporting format, NSI approved data collection codes, and ISE-SAR information sharing and disclosure business rules.

3. ISE-SAR information retained by the OHSP/FC and entered into the shared space will be accessed by or disseminated only to persons within the FC or, as expressly approved by the NSI Program Management Office, users who are authorized to have access and need the information for specific purposes authorized by law or center policy. Access to 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 CTWatch staff 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 FC 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 OHSP and FC for this type of information.

5. ISE-SAR information will not be provided to the public if, pursuant to N.J.S.A. 47:1A1.1, 1.2, 3.a., 5.k., 9, 10, or Legislative findings, or under Executive Order 21, 26 or 69 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.

   See Sec. B-3 Open Public Records Act (OPRA)

6. The CTWatch staff 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, unless otherwise required by law.

J. Disclosure, Correction, and Appeal/Redress

See Sec. B-3 Open Public Records Act (OPRA)

J.1. Mandatory Disclosure and Correction –

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 OHSP/FC or a source agency participating in the NSI may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information. The OHSP/FC'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 or other requestor when, pursuant to N.J.S.A. 47:1A1.1, 1.2, 1.22, 3.a, 5.k., 9, 10 or Legislative Findings or under Executive Order 21, 26 or 69:
   - 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;

- The information is in a criminal intelligence information subject to 28 CFR Part 23 [see 28 CFR § 23.20(e)];
- The information source does not reside with the center;
- The OHSP/FC or user agency did not originate, or does not otherwise have a right to disclose, the information; or
- Other authorized basis for denial under New Jersey law.

3. The individual to whom information has been disclosed will be given reasons if requests for correction(s) are denied by the OHSP/FC or the source agency. The individual will also be informed of the procedure for appeal when the FC or source agency 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 exempt from disclosure, is alleged to be held by the OHSP/FC, and is claimed to have resulted in demonstrable harm to the complainant, the OHSP/FC, as appropriate, will inform the individual of the procedure for submitting and resolving such complaints. Complaints will be received by the OHSP or FC's Privacy Officer at the following address: Maureen Lancaster, NJ OHSP, Phone: 609-584-4349, Email: Maureen.lancaster@ohsp.state.nj.us

2. The Privacy Officer 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, unless otherwise required by law.

3. If the information did not originate with the center, the Privacy Officer will notify the originating agency in writing or electronically within 10 days and, upon request, assist such agency to correct any identified data/record deficiencies, purge the information, or verify that the record is accurate. All ISE-SAR information held by the center that is the subject of a complaint will be reviewed within 30 days and confirmed or corrected/purged if determined to be inaccurate, incomplete, to include incorrectly merged information, or to be out of date. If there is no resolution within 30 days, the center will remove the information from the shared space until such time as the complaint has been resolved. A record will be kept by the center of all ISE-SAR related complaints and the resulting action taken in response to the complaint.

K. Security Safeguards

1. The OHSP's Security Officer is designated and trained to serve as the OHSP's security officer for the NSI.

2. The OHSP/FC will operate in a secure facility protecting the facility from external intrusion. The OHSP/FC will utilize secure internal and external safeguards against network intrusions

of ISE-SAR information. Access to the OHSP/FC's ISE-SAR shared space from outside the facility will be allowed only over secure networks.

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

4. Access to ISE-SAR information will be granted only to OHSP/FC 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 OHSP/FC will, in the event of a data security breach follow applicable state law requirements related to data breach notification requirements set forth in the New Jersey Criminal Justice Information System (CJIS) Guidelines (see Appendix C).

L. Information Retention and Destruction

1. The CTWatch staff will ensure that all ISE-SAR information is reviewed for record retention (validation or purge) in accordance with the time period(s) specified by OHSP/FC policy, (OHSP NJSARS Retention Policy which dictates review and purge after five years), as applicable.

2. The CTWatch will retain ISE-SAR information in the shared space for a sufficient period of time to permit the information to be validated or refuted, its credibility and value to be reassessed, and a "disposition" label (for example, undetermined or unresolved, cleared or unfounded, or under active investigation) assigned so that a subsequent authorized user knows the status and purpose for the retention and will retain the information based on any retention period associated with the disposition label.

3. When ISE-SAR information has no further value or meets the OHSP CTWatch Compliance Unit criteria for purge according to the OHSP NJSARS Retention Policy applicable law or policy, privacy field information, at a minimum, will be purged (see NJSARS Retention Policy).

4. The OHSP/FC policy and procedure for notification of appropriate parties before information is purged is set forth in the (NJSARS Retention Policy).

M. Transparency, Accountability, and Enforcement

M.1. Information System Transparency

1. The OHSP/FC will be open with the public in regard to SAR collection and ISE-SAR information policies and practices. The FC will make its NSI Privacy Policy available upon request and post it on the FC's Web site or Web page.

2. The OHSP 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 CTWatch will have access to an audit trail of inquiries to and information disseminated from the shared spaces.

3. The CTWatch staff 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 a five year periodic and random audits of logged access to the shared spaces in accordance with NSI policy. A record of the audits will be maintained by the OHSP NJSARS System Administrator or other designee of the agency.

4. FC personnel, and source agencies, shall report violations or suspected violations of the OHSP/FC's privacy and CR/CL policy to the OHSP or FC's Privacy Officer.

5. The OHSP NJSARS System Administrator will conduct a five year periodic audit and inspection of the information contained in its ISE-SAR shared space. The audit will be conducted by OHSP staff or an independent auditor, as provided by NSI 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 OHSP/FC in the shared space and any related documentation.

6. The OHSP appointed and trained Privacy Officer will every five years, periodically review the OHSP/FC's Privacy and CR/CL Policy and the OHSP/FC will make appropriate changes in response to changes in applicable law.

M.3. Enforcement

1. The OHSP has and applies procedures (see OHSP NJSARS User Participation Agreement) for enforcement (sanctions) if center personnel, a participating agency, or an authorized user is found to be in noncompliance with the provisions of this policy regarding the gathering, collection, use, retention, destruction, sharing, classification, or disclosure of SAR or ISE-SAR information.

2. The OHSP 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 OHSP further reserves the right to deny access or participation in the NSI to its participating agencies (source or user) that fail to comply with the applicable restrictions and limitations of the OHSP/FC's privacy policy

N. Training

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 OHSP CTWatch and other OHSP/FC employees who have access to SAR or ISE-SAR information. Personnel providing information technology services to the CTWatch and NJSARS application;
- Staff in other public agencies or private contractors, as appropriate, providing SAR and ISE-SAR information technology or related services to the FC;
- Source agency personnel providing organizational processing services for SAR information submitted to the CTWatch; and
- User agency personnel and individuals authorized to access ISE-SAR information who are not employed by the OHSP/FC or a contractor.

1. The OHSP or FC's privacy policy training program will cover:
   - Purposes of the NSI Privacy and CR/CL 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 CTWatch to the shared space;
   - Participating agency responsibilities and obligations under applicable law and policy;
   - 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.

Appendix A - Terms and Definitions

The following is a list of primary terms and definitions that may be used in this document. These terms may also be useful in drafting the definitions section of the center's comprehensive privacy policy.

Access—Data access is being able to get to (usually having permission to use) particular data on a computer. Web access means having a connection to the World Wide Web through an access provider or an online service provider. Data access is usually specified as read-only and read/write access.

With regard to the ISE, access refers to the business rules, means, and processes by and through which ISE participants obtain terrorism-related information, to include homeland security information, terrorism information, and law enforcement information acquired in the first instance by another ISE participant.

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

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

Agency—The OHSP CTWatch and all agencies that access, contribute, and share information in the NJSARS system.

Audit Trail—A generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail—what commands were issued to the system, what records and files were accessed or modified, etc. Audit trails are a fundamental part of computer security, used to trace (albeit usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

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

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

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

Center—Refers to the fusion center and all participating agencies in the center.

Civil Liberties—Fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights—the first ten Amendments to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference. Generally, the term ―civil rights‖ involves positive (or affirmative) government action, while the term ―civil liberties‖ involves restrictions on government.

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

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

Confidentiality—Closely related to privacy but is not identical. It refers to the obligations of individuals and institutions to use information under their control appropriately once it has been disclosed to them. One observes rules of confidentiality out of respect for and to protect and preserve the privacy of others. 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 Information—Information deemed relevant to the identification of and the criminal activity engaged in by an individual who or organization that is reasonably suspected of involvement in criminal activity. Criminal intelligence records are maintained in a criminal intelligence system per 28 CFR Part 23.

CTWatch – Counter Terrorism Watch – where NJSARS information is received, maintained and disseminated under the administration of OHSP. CTWatch is based at the Fusion Center.

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

Data Breach—The unintentional release of secure information to an untrusted environment. This may include incidents such as theft or loss of digital media such as computer tapes, hard drives, or laptop computers containing such media upon which such information is stored unencrypted; posting such information on the World Wide Web or on a computer otherwise accessible from the Internet without proper information security precautions; transfer of such information to a system that is not completely open but is not appropriately or formally accredited for security at the approved level, such as unencrypted e-mail; or transfer of such information to the information systems of a possibly hostile agency or environment where it may be exposed to more intensive decryption techniques.

Data Protection—Encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, use, protection, and disclosure of information.
Disclosure—The release, transfer, provision of access to, sharing, publication, or divulging of personal information in any manner—electronic, verbal, or in writing—to an individual, agency, or organization outside the agency that collected it. Disclosure is an aspect of privacy, focusing on information which may be available only to certain people for certain purposes but which is not available to everyone.

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

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

Fair Information Principles—The Fair Information Principles (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) relates to the ability to prevent, interdict, or disrupt terrorist activity; (c) would improve the identification or investigation of a suspected terrorist or terrorist organization; or (d) would improve the response to a terrorist act.

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

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

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

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

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

Intelligence-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.

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

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

Law Enforcement Information—For purposes of the ISE, law enforcement information means any information obtained by or of interest to a law enforcement agency or official that is both (a) related to terrorism or the security of our homeland and (b) relevant to a law enforcement mission, including but not limited to information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of or response to criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of or response to criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance.

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

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

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

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

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

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

NJSARS – New Jersey Suspicious Activity Reporting System

NJ OHSP – New Jersey Office of Homeland Security and Preparedness

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

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

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

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

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

Personally Identifiable Information—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 location(s) or place(s) (including geographic information systems [GIS] locations, electronic bracelet monitoring information, etc.).

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

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

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

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

Protected Information—For the nonintelligence 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. While not within the definition established by the ISE Privacy Guidelines, protection may be extended to other individuals and organizations by internal federal agency policy or regulation.
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.

For state, local, and tribal governments, protected information may include information about individuals and organizations that is subject to information privacy or other legal protections by law, including the U.S. Constitution; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 23; applicable state and tribal constitutions; and applicable state, local, and tribal laws, ordinances, and codes. Protection may be extended to other individuals and organizations by fusion center or other state, local, or tribal agency policy or regulation.

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

Public does not include:
 Employees of the center or a participating agency.
 People or entities, private or governmental, which assist the center in the operation of the justice information system.
 Public agencies whose authority to access information gathered and retained by the center is specified in law.

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

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

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

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

Retention—Refer to Storage.

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

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

ROIC – Regional Operations Intelligence Center – New Jersey's Fusion Center

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

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

Source Agency—Source agency refers to the agency or organizational entity that originates 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—Defined in the ISE-SAR Functional Standard (Version 1.5) as ―observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity.‖ Examples of suspicious activity include surveillance, photography of sensitive infrastructure facilities, site breach or physical intrusion, cyber attacks, testing of security, etc.

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

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

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

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

Tips and Leads Information or Data—Generally uncorroborated reports or information generated from inside or outside a law enforcement agency that allege or indicate some form of possible

criminal activity. Tips and leads are sometimes referred to as suspicious incident report (SIR), suspicious activity report (SAR), and/or field interview report (FIR) information. However, SAR information should be viewed, at most, as a subcategory of tip or lead data. Tips and leads information does not include incidents that do not have a criminal offense attached or indicated, criminal history records, or CAD data. Tips and leads information should be maintained in a secure system, similar to data that rises to the level of reasonable suspicion.

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

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

Privacy Policy

APPENDIX B

NJSAR's Policies

- User Manual
- Operating Policy
- Compliance Policy
- Retention Policy

APPENDIX C

NJ Laws, Directives, Guidelines Used for Privacy Policy Legal Compliance

- Executive Order #5 (03-16-06)
- Attorney General Memo – Guidelines for Dissemination of the NJ Public and Law Enforcement (10-09-07)
- Attorney General Guidelines on Collection, Handling, Storage and Dissemination of Intelligence in NJ (03/09/05)
- Domestic Security Preparedness Task Force Act
- U.S. Constitution
- NJ OPRA
- NJ Law Against Discrimination
- CJIS Policies