Northeast Ohio Regional Fusion Center Privacy Policy

5.1 Purpose Statement

The Northeast Ohio Regional Fusion Center (hereinafter referred to as the "NEORFC") will facilitate effective information and intelligence sharing to prevent, detect, deter, and mitigate threatened or actual terrorist events, working with and supporting local, state and federal governmental agencies, public and private sectors, and the citizens of Ohio.

The NEORFC has created and will abide by this Privacy Policy in order to ensure that its information sharing and analysis does not violate any individual privacy rights, civil rights, civil liberties, and other protected interests. This Policy sets forth guidelines and procedures, which comply with state and federal privacy laws that NEORFC personnel must follow in their furtherance of the NEORFC's mission.

5.2 Policy Applicability and Legal Compliance

1. All NEORFC personnel, participating agency personnel, personnel providing information technology services to the agency, private contractors, and other authorized users will comply with the NEORFC's privacy policy concerning the information the center collects, receives, maintains, archives, accesses, or discloses to center personnel, governmental agencies (including Information Sharing Environment [ISE] agencies), and participating criminal justice and public safety agencies, as well as to private contractors and the general public.

2. The NEORFC will provide a printed copy of this policy to all agency and non-agency personnel 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 the provisions it contains.

3. All NEORFC personnel, participating agency personnel, personnel providing information technology services to the agency, private contractors, and other authorized users will comply with the laws of the State of Ohio (R.C. §§109.57, 149.43, 149.433, 2953.32, 2953.52, 5502.03, 5503.10), the Constitution of the State of Ohio (Article I, §§1, 3, 11) and the Constitution of the United States (Bill of Rights, 1st Amendment, 4th Amendment, 14th Amendment). Criminal Intelligence Data shall be kept in accordance with 28 C.F.R. Part 23.

4. The NEORFC has adopted internal operating policies that are in compliance with the aforesaid applicable laws protecting privacy, civil rights, and civil liberties. *See also* Privacy Act (5 U.S.C. 552a), Driver's Privacy Protection Act (18 U.S.C. §2721), Wiretap Statutes (18 U.S.C. §2510, et seq.; 47 U.S.C. §605), 42 U.S.C. §1983.

5.3 Governance and Oversight

1. Primary responsibility for the operation of the NEORFC, 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 Director of the NEORFC.

2. The NEORFC shall utilize a privacy oversight team that liaises with community privacy advocacy groups to ensure that privacy, civil rights, and civil liberties are protected as provided in this policy and by the center's implementing processes and procedures. The privacy oversight team is guided by a center-designated, trained privacy officer. In conjunction with the Director, the privacy oversight team will annually review the policy and make recommendations for changes to the Director in response to changes in applicable law, implementation experience, and the results of audits and inspections. The privacy oversight team and the privacy officer are

appointed by the Director.

3. The privacy officer 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, serve as the center's privacy liaison for the Information Sharing Environment, and, in conjunction with the Director, ensure that privacy protections are implemented, including the ISE privacy Guidelines, through training, business process changes, and system designs that incorporate privacy enhancing technologies. The privacy officer can be contacted at the following address: Northeast Ohio Regional Fusion Center, ATTN: Privacy Officer, 1300 Ontario Street, Suite 935, Cleveland, Ohio, 44113.

4. The NEORFC's privacy officer ensures that enforcement procedures and sanctions outlined in 5.16 Enforcement are adequate and enforced.

5.4 Terms & Definitions

Definitions of terms contained within this policy are contained in "Appendix A, Terms and Definitions".

5.5 Information

1. The NEORFC will seek or retain information that:

   - Is based upon a criminal predicate or possible 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, 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 (including topical searches); and
   - The source of the information is reliable and verifiable or limitations on the quality of the information are identified; and
   - The information was collected in a fair and lawful manner, with the knowledge and consent of the individual, if appropriate.

   The NEORFC will also retain information that does not reach a level of reasonable suspicion, such as tips and leads or suspicious activity reports (SARs). Refer to 5.5.7 for the center's practices and procedures for this type of information.

2. The NEORFC will not seek or retain information about individuals or organizations solely on the basis of the following: religious, political, or social views or activities; participation in a particular non-criminal organization or lawful event; or race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation.

3. The NEORFC applies labels to all center-owned information to indicate to the accessing authorized user that:

   - The information pertains to "protected information" to include 'personal data" on any individual (see Appendix A, Terms and Definitions) and, to the extent expressly provided in this policy, includes organizational entities.
   - The information is subject to R.C. §§149.43, 149.443 and/or 5502.03, and all applicable state and federal laws restricting access, use, or disclosure of information.

Information obtained from other agencies will remain in its original format.

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

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

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

    Labels include "Law Enforcement" (Read, Write, and Modify any material) and "Non-Law Enforcement" (Read, Write, and Modify only non law-enforcement material). The granting of access shall be restricted to the Director of the NEORFC.

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

    - New information is added that has an impact on access limitations or the sensitivity of disclosure of the information; or
    - There is a change in the use of the information affecting access or disclosure limitations.

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

    - Prior to allowing access to or dissemination of the information, 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 categorize the information as unsubstantiated or uncorroborated after attempts to validate or determine the reliability of the information fail.
    - Store the information using the same storage method used for data that rises to the level of reasonable suspicion, but in a file clearly separate from criminal intelligence, and includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information.
    - Allow access to or disseminate the information using the same (or a more restrictive) access or dissemination method that is used for data that rises to the level of reasonable suspicion (for example, "need-to-know" and "right-to-know" access or dissemination). Personnel must sign and adhere to the NEORFC's Privacy Policy.
    - Regularly provide access to or disseminate the information in response to an interagency inquiry for law enforcement, homeland security, or public safety and analytical purposes or when credible information indicates potential imminent danger to life or property.
    - Retain information for up to one year to work a tip or lead or SAR information to determine

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

- Adhere to and follow the center's physical, administrative, and technical security measures that are in place for the protection and security of tips and leads information. Tips, leads, and SAR information will be secured in a system that is the same or similar to, but separate from, the system that secures data that rises to the level of reasonable suspicion.
- The NEORFC incorporates the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious activities and incidents (SAR process) into existing processes and systems used to manage other crime-related information and criminal intelligence. All SAR data within the NEORFC will be clearly identified as such and will be stored in a separate database than criminal intelligence, but will have the same securities as that of criminal intelligence.

8. The NEORFC 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. Furthermore, the center will provide notice mechanisms, including but not limited to metadata and labeling of fields, 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.

9. The NEORFC requires certain basic descriptive information to be entered and electronically associated with each piece of data (or content) that is to be accessed, used, and disclosed, such as:

    - The name of the originating department, component, and subcomponent.
    - If applicable, the name of the center's justice information 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 person to whom questions regarding the information should be directed.

10. The NEORFC will apply specific labels and descriptive metadata to information that will be accessed and disseminated to clearly indicate all legal restrictions on information sharing based on information sensitivity or classification. Metadata fields will include: the legal authority, classified information categories, indicator of special clearance required, special access processes, caveats, polygraphs, non-disclosure agreements, and sensitive but unclassified labels.

11. The NEORFC will keep a record of the source of all information retained by the center.

5.6 Acquiring and Receiving Information

1. Information gathering and investigative techniques used by the NEORFC and affiliated agencies will comply and adhere to the following regulations and guidelines:

    - The center will follow 28 CFR Part 23 with regard to criminal intelligence, including the requirement for reasonable suspicion of involvement in criminal activity and limiting dissemination of criminal intelligence information to agencies and users with a "need to know" and a "right to know" the information (See Definitions. Appendix A).
    - The center will adhere to the Organization for Economic Cooperation and Development's (OECD) *Fair Information Practices* (However, under certain circumstances, there may be exceptions to the *Fair Information Practices*, based, for example, on authorities similar to

those provided in the Privacy Act, State Local and Tribal (SLT) law, or agency policy).
- The center will adhere to applicable criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) *National Criminal Intelligence Sharing Plan* (NCISP).
- The center will make every reasonable effort to insure that it complies with R.C. Chapter 1347 (Duties of state and local agencies maintaining personal information systems), as well as the U.S. and Ohio constitutions and any other laws or regulations that apply to privacy, civil rights, and civil liberties protections for multi-jurisdictional intelligence and information databases.

2. The NEORFC's SAR and tips and leads process provides for human review and vetting to ensure that information is both legally gathered and, where applicable, determined to have a potential terrorism nexus. Law enforcement officers, NEORFC staff, participating agencies, and participating personnel will be trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism.

3. The NEORFC will identify SAR information related to terrorism that is eligible for sharing in the ISE using the two-step process set forth in the ISE-SAR Functional Standard. Participating personnel will be responsible for vetting and updating information posted to the ISE-SAR shared space by the center.

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

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

6. Agencies which participate in the NEORFC and which provide information to the center are governed by the laws and rules governing those individual agencies, as well as by applicable federal and state laws, including those cited in 5.6.1.

7. The NEORFC 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 and which is not based on misleading information collection practices.

8. The NEORFC will not directly or indirectly receive, seek, accept, or retain information from:

    - An individual or information provider who has obtained information illegally; or
    - An individual or information provider that may or may not receive a fee or benefit for providing the information, except as expressly authorized by law or center policy.

5.7 Information Quality Assurance

1. The NEORFC will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources of information; accurate; current; complete, including the relevant context in which it was sought or received and other related information; and merged with other information about the same individual or organization only when the applicable standard [Refer to Section 5.9 Merging Information From Multiple Sources] has been

met.

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

3. The NEORFC 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.

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

5. The NEORFC will conduct periodic data quality reviews of information it originates or retains for dissemination and make every reasonable effort to ensure that information will be corrected or deleted from the system when the center learns that the information is unreliable or invalid; the source of the information did not have authority to gather the information or to provide the information to the center; or the source used prohibited means to gather the information, except when the source did not act as an agent to a bona fide law enforcement officer.

6. Center participating agencies are responsible for the quality and accuracy of the data accessed by or provided to the center. Center participating agencies providing data remain the owners of the data contributed. The NEORFC will advise the appropriate data owner, in writing (including electronically), if its data is found to be inaccurate, incomplete, out of date, or unverifiable.

7. The NEORFC will use written or documented electronic notification to inform recipient agencies when information previously provided by the NEORFC is deleted or changed by the center because the information is determined to include incorrectly merged information, be out of date, unverifiable, or to lack adequate context such that the rights of the individual may be affected.

5.8 Collation and Analysis

1. Information sought or received by the NEORFC or accessed from other sources under Section 5.5.1. will be analyzed, for purposes set forth in Section 5.8.2. of this policy, by qualified individuals who have successfully completed a background check and appropriate security clearance, if applicable, and have been selected, approved, and trained accordingly.

2. Information will be analyzed only to further crime prevention, enforcement, force deployment, or prosecution and to provide intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal (including terrorist) activities or who may be a threat to public safety.

3. The NEORFC requires that all analytical products be reviewed and approved by the Privacy Officer [or the privacy officer's designee] to ensure that they provide appropriate privacy, civil rights, and civil liberties protections prior to dissemination or sharing by the center.

5.9 Merging Information from Multiple Sources

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

2. If the matching requirements are not fully met but there is an identified partial match, the

information may be associated if accompanied by a clear statement that it has not been adequately established that the information relates to the same individual or organization.

5.10 Sharing and Disclosure

1. Credentialed, role-based access criteria (See Section 5.5.4) will be used, as appropriate, to control:

   - What information a class of users can have access to;
   - What information a class of users can add, change, delete, or print; and
   - To whom the information can be disclosed and under what circumstances

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

2. Access to information retained by the NEORFC will only be provided *to authorized persons within the NEORFC or in other governmental agencies* who are engaged in 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 whom the person is working. An audit trail will be kept of access by or dissemination of information to such persons.

3. Participating agencies may not disseminate NEORFC information without approval from the originator of the information.

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

5. Information gathered and retained by the NEORFC may be disseminated *for specific purposes* upon request by persons authorized by law to have such access and only for those users or purposes specified in the law.

   - An audit trail will be kept for at least three years, which will include requests for access and information disseminated to each person.

6. Information gathered and retained by the NEORFC 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 agency mission and is not excepted from disclosure by law, and it may only be disclosed in accordance with the law and procedures applicable to the NEORFC for this type of information or when there is a legitimate need. An audit trail will be kept of all requests and of what information is disclosed to a member of the public. See Section 5.12 for the NEORFC redress policy.

7. Information gathered and retained by the NEORFC ***will not*** be:

   - Sold, published, exchanged, or disclosed for commercial purposes;
   - Disclosed or published without prior notice to the contributing agency that it is subject to re-disclosure or publication; or

- Disseminated to unauthorized persons.

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

   - Public records required to be kept confidential by law are exempted from disclosure requirements under R.C. §§149.43, 149.433, and 5502.03.
   - Investigatory records of law enforcement agencies are exempted from disclosure requirements under R.C. Sections §149.43. However, certain law enforcement records must be made available for inspection and copying if not exempted from disclosure under R.C. §149.43.
   - 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 R.C. §§149.43,149.433, and 5502.03. This includes a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism, agricultural terrorism, vulnerability assessments, risk planning documents, needs assessments, and threat assessments under R.C. §§149.433 and 5502.03.
   - Protected federal, state, local, or tribal records, which may include records owned or controlled by another agency.
   - Information that meets the definition of "classified information" as that term is defined in the National Security Act, Public Law 235, Section 606, and in accord with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010.
   - Information prohibited from being disclosed pursuant to court order.

9. The NEORFC staff shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.

5.11 Disclosure to the Subject of a Record

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 is entitled to know the existence of and to review the information about him or her that has been gathered and retained by the NEORFC. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information by contacting the Privacy Officer at the following address: Northeast Ohio Regional Fusion Center, ATTN: Privacy Officer, Justice Center Complex, 1 West Lakeside Avenue, Cleveland, Ohio, 44113. The NEORFC'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. If the exemptions below do not apply, and information exists that was provided from another agency, the NEORFC will refer the request to that agency and assist and facilitate with the communication between the individual and the agency.

   - The existence, content, and source of the information *will not* be made available to an individual when:
   - Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution (R.C. §§ 109.57, 149.43, 1347.08, 1347.12, 5502.03);
   - Disclosure would endanger the health or safety of an individual, organization, or community (e.g., R.C. §§149.433, 1347.12; *Kallstrom v. City of Columbus*, 165 F. Supp. 2d 686, S.D. Ohio, 2001);
   - The information is in a criminal intelligence system (28 C.F.R. Part 23);
   - The information is protected by State or Federal statute (e.g., R.C. §§ 109.57, 149.43, 149.433, 1347.08, 1347.12, 5502.03);

- The information source does not reside with the NEORFC; or the NEORFC does not own or have a right to disclose the information (i.e., Third-Party Rule).

5.12 Complaints & Corrections

1. If an individual has complaints or objections to the accuracy or completeness of information retained about him or her *within a system under the center's control*, and such information is not exempt under Section 5.11.2, the NEORFC will inform the individual of the following procedure for submitting complaints or requesting corrections:

   - Submit a written request to the NEORFC, Director, at the following address: Northeast Ohio Regional Fusion Center, ATTN: Complaints and Corrections, Justice Center Complex, 1 West Lakeside Avenue, Cleveland, Ohio, 44113, to investigate the current status of information about the individual.
   - The NEORFC will, within a reasonable period of time, make a reasonable investigation with the providing agency to determine whether the disputed information is accurate, relevant, timely and complete, and will notify the individual of the results of the investigation.
   - The NEORFC will delete any information that it cannot verify or that it finds to be inaccurate.
   - If the investigation reveals that the information is accurate, relevant, timely and complete, the NEORFC shall include within the system a notation that the individual disputes the information and summarize the individual's statement of his position on the disputed information.

   A record will be kept of all complaints and requests for corrections.

2. If the information does not originate with the center, the requestor will be referred to the originating agency, if appropriate or required, or the center will notify the source agency of the request and its determination that disclosure **by the center** or referral **of the requestor** to the source agency was neither required nor appropriate under applicable law. When the complaint pertains to the correction of a record that has been disclosed to the complainant, the originating agency must either consent to the correction and remove the record, or assert a basis for denial in accordance with R.C. Chapter 1347. This must be done in sufficient time to permit compliance with deadlines found within R.C. Chapter 1347. A record will be kept of all complaints and requests for corrections. If an individual has a complaint with regard to the accuracy or completeness of terrorism-related protected information that:

   - Is exempt from disclosure.
   - Has been or may be shared through the ISE,
   - Is held by the NEOFC and
   - 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 Northeast Ohio Regional Fusion Center, ATTN: Privacy Officer, 1300 Ontario Street, Suite 935, Cleveland, Ohio, 44113.

   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 of all complaints and requests for corrections.

3. To delineate ISE agency information from other contributing agency's data, the NEORFC maintains records of the ISE originating agencies the center has access to, as well as audit logs, and employs system mechanisms whereby the source (or owning agency, including ISE agencies) is identified within the information record.

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

5.13 Security Safeguards

1. The NEORFC's Security Officer will receive appropriate training and will be designated by Ohio Homeland Security's Executive Director or the NEORFC's Director.

2. The NEORFC will operate in a secure facility protecting the facility from external intrusion. The NEORFC will utilize secure internal and external safeguards against network intrusions. Access to NEORFC databases from outside the facility will only be allowed over secure networks.

3. The NEORFC will secure tips, leads and SAR information in a separate repository system that is the same as or similar to the system that secures data rising to the level of reasonable suspicion.

4. The NEORFC will store information in a manner that it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions as designated by the Director of the center.

5. Access to center information will only be granted to center personnel whose position and job duties with the center require such access and the individual has successfully completed a background check and appropriate security clearance, if applicable, and has been selected, approved, and trained accordingly.

6. Queries made to the NEORFC data applications will be logged in the data system and will identify the user initiating the query.

7. The NEORFC will utilize logs to maintain audit trails of requested and disseminated information. Records of dissemination shall be kept with the original data entry.

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

9. The NEORFC will notify an individual about whom personal information was or is reasonably believed to have been breached or obtained by an unauthorized person and access to which threatens the physical, reputational, or financial harm to the person. The notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or any measures necessary to determine the scope of the release of information and, if necessary, to reasonably restore the integrity of any information system affected by this

release. (See R.C. §1347.12).

5.14 Information Retention and Destruction

1. All criminal intelligence information will be reviewed for record retention (validation or purge) at least every five (5) years, as provided by 28 C.F.R. Part 23. Additionally, all suspicious activity report (SAR) data will have a retention period of five (5) years, after which point the data will be either validated or purged.
2. When information (including printed, handwritten or electronic) has no further value or meets the criteria for removal according to the NEORFC's retention and destruction policy, it will be purged, destroyed, and deleted, or returned to the submitting source. The NEORFC will purge, destroy, or delete information or return it to the source, unless it is updated and validated, every five (5) years.
3. Permission to destroy or return information or records will be presumed if the applicable information is not updated, within the specified time period, as per item (2), above.
4. Notification of proposed destruction or return of records may or may not be provided to the contributor, depending on the relevance of the information.
5. A record of information to be reviewed for retention will be maintained by the NEORFC, and for appropriate system(s), notice will be given to the submitter at least 30 days prior to the required review date.

5.15 Accountability and Enforcement

A. Information System Transparency

1. The NEORFC will be open with the public in regard to information and intelligence collection practices. The NEORFC's privacy policy will be provided to the public for review and made available upon request. Information on how to request the policy will be posted on the Ohio Homeland Security website at http://www.neorfc.us/.
2. The NEORFC Privacy Officer and City of Cleveland Law Department will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s). Inquiries and complaints can be addressed to: Northeast Ohio Regional Fusion Center, ATTN: Privacy Officer, Justice Center Complex, 1 West Lakeside Avenue, Cleveland, Ohio, 44113

B. Accountability

1. Queries made to the NEORFC data applications will be logged into the data system identifying the user initiating the query.
2. The NEORFC log will be utilized to maintain an audit trail of requested or disseminated information. An audit trail will be maintained for the life cycle of the applicable record.
3. The NEORFC will provide a copy of this policy to all agency and non-agency personnel who provide services and will require written acknowledgement of receipt of this policy and agreement of compliance to this policy and the provisions it contains.
4. The NEORFC will adopt and follow procedures and practices by which it can ensure and

evaluate the compliance of users with their systems, in provisions of this policy and applicable law. This will include logging access of these systems and periodic auditing of these systems, as to not establish a pattern of the audits. These audits will be mandated at least quarterly and a record of the audit will be maintained by the Director (or designee) of the center.

5. The NEORFC's personnel or other authorized users shall report violations or suspected violations of center policies relating to protected information to the center's Privacy Officer.

6. The NEORFC will annually provide for the conduct of an audit and inspection of the information contained in its information and criminal intelligence systems. The audit will be conducted by a designated, independent panel. This independent panel has the option of conducting a random audit, without announcement, at any time, and without prior notice to the NEORFC. This audit will be conducted in such a manner so as to protect the confidentiality, sensitivity, and privacy of the center's criminal intelligence system.

7. The NEORFC's Privacy oversight team will annually review and update the provisions protecting privacy, civil rights, and civil liberties contained within this policy and recommend appropriate changes in response to changes in applicable law, implementation experience, and the results of audits and inspections. (See Section 5.3.2).

5.16 Enforcement

1. If NEORFC personnel, participating agency personnel, personnel providing information technology services to the agency, private contractors, or an authorized user is found to be not complying with the provisions of this policy regarding the collection, use, retention, destruction, sharing, classification, or disclosure of information, the Director of the NEORFC will:

   - Suspend or discontinue access to information by the authorized user or user agency;
   - Suspend, demote, transfer, or terminate the person, as permitted by applicable DPS and/or NEORFC policies;
   - Apply administrative actions or sanctions as provided by Department of Public Safety rules and regulations or as provided in agency personnel policies;
   - If the user is from an agency external to the center, request that the relevant agency, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions; or
   - Refer the matter to the City of Cleveland, Division of Police, Cuyahoga County Sherriff's Office, and/or the Federal Bureau of Investigation for criminal prosecution, as necessary, to effectuate the purposes of the policy.

2. The NEORFC 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.

5.17 Training

1. The NEORFC will require the following individuals to participate in training programs regarding the implementation of and adherence to the privacy, civil rights, and civil liberties policy:

   - All assigned personnel of the center,

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

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

3. The NEORFC'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 NEORFC;
    - 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 infraction accessible within or through the agency;
    - Mechanisms for reporting violations of center privacy-protection policies; and the nature and possible penalties for policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.
    - Originating and participating agency responsibilities and obligations under applicable law

Appendix A:
Terms and Definitions

The following is a list of primary terms and definitions used throughout this policy. These terms are useful in understanding the meaning of terms within in this 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. For data access, access is usually specified as read-only access 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 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.

Agency/Center—Agency/Center refers to the NEORFC and all participating local, county, state agencies of the NEORFC.

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

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

Civil Rights—The term "civil rights" is used to imply that the state has a role in ensuring 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 upon government to promote equality. More specifically, they are the rights to personal liberty guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments and by acts of Congress.

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

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

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

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

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

Data—Inert symbols, signs, or measures.

Data Breach—The unintentional release of secure information to an untrusted environment.

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

Disclosure—The release, transfer, provision of access to, or divulging of personally identifiable information in any other manner—electronic, verbal, or in writing—to an individual, agency, or organization outside of the agency who collected it. Disclosure is a subset 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 disk 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, transmission over the Internet, intranet, extranet, leased lines, dial-up lines, private networks, telephone voice response, and faxback systems. It does not include faxes, telephone calls, video teleconferencing, or messages left on voice mail.

Fair Information Practices—The Fair Information Practices (FIPs) are contained within the Organization for Economic Cooperation and Development’s (OECD) Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data. These were developed around commercial transactions and the Trans-Border 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 could 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 could be either resolved or unresolved. The record is maintained per statute, rule, or policy.

Homeland Security Information—As defined in Section 482(f)(1) of the Homeland Security Act, homeland security information means any information possessed by a federal, state, local, or tribal agency that relates to (A) a threat of terrorist activity; (B) the ability to prevent, interdict, or disrupt terrorist activity; (C) the identification or investigation of a suspected terrorist or terrorist organization or any person, group, or entity associated with or assisting a suspected terrorist or terrorist organization; or (D) a planned or actual 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 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 compound of such data as a given and family name, date of birth, and address. An organization's identification process comprises the acquisition of the relevant identifying information.

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

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

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

Information Sharing Environment (ISE) Suspicious Activity Report (SAR) (ISESAR)—An ISE-SAR is a

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

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

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 or 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 they are authorized to perform.

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

Maintenance of Information—The maintenance of information applies to all forms of information storage. This would include electronic systems (for example, databases) and non-electronic storage systems (for example, filing cabinets). To meet access requirements, an organization is not required to create new systems to maintain information or 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 content. 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 upon the type of information and 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.

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

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

Participating Agency Personnel – Individuals who have signed participating agreements with the Ohio Department of Public Safety and have direct access to the NEORFC's storage of databases, electronic documents and other files.

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

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

Personally Identifiable Information—Personally identifiable information is one or more pieces of information that when considered together or when considered in the context of how it is presented or how it is gathered is 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 a United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, 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 State citizens and lawful permanent residents.

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

Privacy Policy—A privacy policy is a written, published statement that articulates the policy position of an organization on how it handles the personally identifiable 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 agency will adhere to those legal requirements and agency policy

determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well-developed and implemented privacy policy uses justice entity resources wisely and effectively; protects the agency, the individual, and the public; and promotes public trust.

Privacy Protection—This is a process of finding appropriate balances between privacy and multiple competing interests, such as justice information sharing.

Protected Information—protected information includes personal data or information that is subject to information privacy or other legal protections under the U.S. Constitution and the Ohio constitution; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 23; applicable state and tribal constitutions; and state, local and tribal laws, ordinances, and codes. Protection may also be extended to organizations by center policy or state, local or tribal law.

Public—Public includes:

Any person and any for-profit or nonprofit entity, organization, or association;

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

Public does not include:

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

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

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

Redress—Internal procedures to address complaints from persons regarding protected information about them that is under the agency's control.

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

Retention—Refer to "Storage."

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

Right to Privacy—The possible right to be let alone, in the absence of some reasonable public interest in 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 that right.

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

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

Storage—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 homeland security information, terrorism information, and law enforcement information by both the originator of the information and any recipient of the information.

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

Suspicious Activity Reports (SAR)—The official documentation of observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity. At the federal level, there are two types of SAR information: (1) Information Sharing Environment SAR information that pertains to terrorism information; and (2) Banking Secrecy Act SAR information that pertains to suspicious banking activity and is required to be completed by financial institutions. Suspicious activity reports (SAR) are meant to offer a standardized means for feeding information repositories or data mining tools. Any patterns identified during SAR data mining and analysis may be investigated in coordination with the reporting agency and the state designated fusion center. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities. Nor are they designed to support interagency calls for service.

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

892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. § 482(f)(1)); and (2) law enforcement information relating to terrorism or the security of our homeland). Such additional information includes intelligence information. Weapons of Mass Destruction (WMD) information is defined and included in the definition of "terrorism information" by P.L. 110-53.

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

A tip or lead can result from a variety of sources, including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information has some suspicion or mere suspicion attached to it, but has not been evaluated and vetted.

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

User or Authorized User—An individual – including all NEORFC personnel, participating agency personnel, personnel providing information technology services to the NEORFC, private contractors, and other authorized users -- 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
Federal Laws Relevant to Seeking, Retaining, and Disseminating Justice Information

Excerpt from: U.S. Department of Justice's (DOJ's) Privacy, Civil Rights, and Civil Liberties Policy Templates for Justice Information Systems

The U.S. Constitution is known as the primary authority that applies to federal as well as state, local, and tribal (SLT) agencies. State constitutions cannot provide fewer privacy and other civil liberties protections than the U.S. Constitution but can (and many do) provide enhanced privacy and other civil liberties protections.

Civil liberties protections are primarily founded in the Bill of Rights. They include the basic freedoms, such as free speech, assembly, and religion; freedom from unreasonable search and seizure; due process; etc. The relationship of these fundamental rights to the protection of privacy, civil rights, and other civil liberties in the Information Sharing Environment is explored in a key issues guidance paper titled *Civil Rights and Civil Liberties Protection*, which is available on the Program Manager (PM) for the Information Sharing Environment (PM-ISE) Web site at www.ise.gov.

Statutory civil rights protections in the U.S. Constitution may, in addition, directly govern state action. These include the Civil Rights Act of 1964, as amended; the Rehabilitation Act of 1973; the Equal Educational Opportunities Act of 1974; the Americans with Disabilities Act; the Fair Housing Act; the Voting Rights Act of 1965; and the Civil Rights of Institutionalized Persons Act.

Federal laws, Executive Orders, regulations, and policies directly affect agencies'/centers' privacy policies. While SLT agencies may not be generally bound directly by most statutory federal privacy and other civil liberties protection laws in the information collection sharing context, compliance may be required **indirectly** by funding conditions (e.g., 28 CFR Parts 20, 22, and 23 or the Health Insurance Portability and Accountability Act [HIPAA]); operation of the Commerce Clause of the U.S. Constitution (e.g., Electronic Communications Privacy Act of 1986); or a binding agreement between a federal agency and an SLT agency (e.g., a memorandum of agreement or memorandum of understanding). Where relevant or possibly relevant, agencies/centers are advised to list these laws, regulations, and policies, noting those that may potentially affect the sharing of information, including sharing terrorism-related information in the Information Sharing Environment.

The development of a privacy, civil rights, and civil liberties policy is primarily designed for center personnel and authorized users to ensure that they are aware of the legal and privacy framework within which they and the center must operate. If the applicability and requirements of various laws, regulations, or sharing agreements are not spelled out or referenced in an

center privacy policy, staff and user accountability is greatly diminished, mistakes are made, privacy violations occur, and the public's (and other agencies') confidence in the ability of the center to protect information and intelligence is compromised. When staff members know the rules through sound policy and procedure communicated through ongoing training activity, information sharing is enhanced.

Following is a partial listing of federal laws that should be reviewed when developing a privacy policy for a justice information system. The list is arranged in alphabetical order by popular name.

Brady Handgun Violence Prevention Act, 18 U.S.C. §§ 921, 922, 924, and 925A, United States Code, Title 18, Part I, Chapter 44, §§ 921, 922, 924, and 925A

Computer Matching and Privacy Act of 1988, 5 U.S.C. § 552a(a), United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a(a); see also Office of Management and Budget, Memorandum M-01-05, "Guidance on Interagency Sharing of Personal Data–Protecting Personal Privacy," December 20, 2000

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

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

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

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

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

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

Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2522, 2701–2709, United States Code, Title 18, Part I, Chapter 119, §§ 2510–2522, 2701–2709, and 3121–3125, Public Law 99-508

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

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

Subchapter I, § 1983

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

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

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

HIPAA, Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164; Code of Federal Regulations, Title 45, Parts 160 and 164

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

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

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

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

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

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

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

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

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

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

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