NORTHERN VIRGINIA REGIONAL INTELLIGENCE CENTER
SOP 5 – Privacy, Civil Rights, Civil Liberties Policy

TABLE OF CONTENTS

A. Purpose

1. The mission of the Northern Virginia Regional Intelligence Center (NVRIC) is to gather, evaluate, analyze, and disseminate information and intelligence data regarding all criminals and all hazards, to include terrorist activity in the Northern Virginia area while following Fair Information Practices to ensure the rights and privacy of individuals and organizations. This includes implementing appropriate privacy and civil liberties safeguards as outlined in the principles of the Privacy Act of 1974, as amended, to ensure that privacy and other legal rights of individuals and organizations are protected (see definitions of "Fair Information Practice Principles" (FIPPs) and "Protected Information" in Appendix A.

2. The NVRIC recognizes the importance of ensuring the protection of individual constitutional rights, civil liberties, civil rights, and privacy interests throughout the intelligence process. The purpose of this policy is to promote those rights and interests in the operation of the NVRIC and user conduct that complies with applicable federal, state, local, and tribal laws as found in Appendix B and assists the center and its users in:
    - Increasing public safety and improving national security.
    - Minimizing the threat and risk of injury to specific individuals.
    - Minimizing the threat and risk of physical or financial injury to law enforcement and others responsible for public protection, safety, or health.
    - Minimizing the threat and risk of damage to personal property.
    - Protecting individual privacy, civil rights, civil liberties, and other protected interests.
    - Protecting the integrity of the criminal investigations, criminal intelligence, and justice system processes and information.
    - Minimizing reluctance of individuals or groups to use or cooperate with the justice system.
    - Supporting the role of the justice system in society.
    - Promoting governmental legitimacy and accountability.
    - Not unduly burdening the ongoing business of the justice system.
    - Making the most effective use of public resources allocated to public safety agencies.

B. Policy Applicability and Legal Compliance

1. All NVRIC personnel, participating agency personnel, personnel providing information technology services to the center, staff members in other public agencies and other private contractors providing services to the center, and other authorized users who are not employed by the center or contract agency will comply with the center's privacy, civil rights, civil liberties policy (P/CRCL). This

policy applies to information the center gathers or collects, receives, maintains, stores, accesses, discloses, or disseminates to center personnel, governmental agencies (including Information Sharing Environment (ISE) participating centers and agencies), and participating justice and public safety agencies, as well as to private contractors, and private entities, and the general public.

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

3. All NVRIC personnel, participating agency personnel, personnel providing information technology services to the center, private contractors, agencies from which center information originates, and other authorized users will comply with applicable laws protecting P/CRCL, including, but not limited to those provided in Appendix B.

4. The NVRIC has adopted internal operating policies that are in compliance with applicable law protecting privacy, civil rights, and civil liberties including, but not limited to Appendix B, and not in conflict with the existing Memorandum of Understanding with the Department of Justice, Federal Bureau of Investigation and the signatories through the Advisory Board.

C. Governance and Oversight

1. Primary responsibility for the operation of the NVRIC, its justice systems, operations, and coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing, disclosure, or dissemination of information; and the enforcement of this policy is assigned to the Director of the center or his/her designee.

2. The NVRIC is guided by an advisory board with the stakeholders to ensure that privacy and civil rights are protected as provided in this policy and by the center's information gathering and collection, retention, and dissemination processes and procedures. The committee, in consultation with a Fairfax County attorney, will annually review and update the policy in response to changes in law and implementation experience, including the results of audits and inspections.

3. The NVRIC's Privacy Officer is appointed by the Director of the center. The Privacy Officer receives reports regarding alleged errors and violations of the provisions of this policy, receives and coordinates complaint resolution under the

center's redress policy, and serves as the liaison for the Information Sharing Environment, ensuring that privacy protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy enhancing technologies. The Privacy Officer can be contacted at the following address: Fairfax County Police Department 12099 Government Center Parkway, Fairfax, Virginia 22035 or FCPDNVRIC@fairfaxcounty.gov.

4. The NVRIC's Privacy Officer, in coordination with the Director, ensures that enforcement procedures and sanctions outlined in Section N are adequate and enforced.

D. Definitions

For a listing of primary terms and definitions used in this Policy, refer to Appendix A, Terms and Definitions.

E. Information

1. The NVRIC will seek or retain information that:
   - Is based on a possible or probable threat to public safety or the enforcement of the criminal law, or
   - Is based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal (including terrorist) conduct or activity, or
   - Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime, or
   - Is useful in crime analysis or in the administration of criminal justice and public safety (including topical searches), and
   - The source of the information is reliable and verifiable or limitations on the quality of the information are identified, and
   - The information was collected in a fair and lawful manner, with the knowledge and consent of the individual, if appropriate.
   - The center may retain protected information that is based on a level of suspicion that is less than "reasonable suspicion," such as tips and leads or suspicious activity report (SAR) information, subject to the policies and procedures specified in this policy.

2. In accordance with applicable laws, guidance, and regulations, the NVRIC will not seek or retain and will inform information-originating agencies not to submit

information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, national origin, ages, disabilities, genders, gender identities, or sexual orientations.

When participating on a federal law enforcement task force or when documenting a SAR or an ISE-SAR in the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI), race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity must not be considered as factors creating suspicion. However, those attributes may be documented in specific suspect descriptions for identification purposes.

3. The NVRIC applies labels to center-originated information (or ensures that the originating agency has applied labels) to indicate to the accessing authorized user that:
   - The information is "protected information" to include "personal information" (as defined in Appendix A) on any individual and, to the extent expressly provided in this policy, including organizational entities.
   - The information is subject to laws restricting access, use, or disclosure, located in Appendix B.

4. The NVRIC personnel will, upon receipt of information, assess the information to determine or review its nature, usability, and quality. Personnel will assign categories to the information (or ensure that the originating agency has assigned categories to the information) to reflect the assessment, such as:
   - Whether the information consists of tips and leads data, suspicious activity reports (SARs), criminal history, intelligence information, case records, conditions of supervision, case progress, or other information category.
   - The nature of the source as it affects veracity (for example, anonymous tip, trained interviewer or investigator, public record, private sector).
   - The reliability of the source (for example, reliable, usually reliable, unreliable, unknown).
   - The validity of the content (for example, confirmed, probable, doubtful, cannot be judged).

5. At the time a decision is made by the NVRIC to retain information; it will be labeled appropriately, to the maximum extent feasible, pursuant to applicable limitations on access and sensitivity of disclosure to:
   - Protect confidential sources and police undercover techniques and methods.
   - Not interfere with or compromise pending criminal investigations.

- Protect an individual's right of privacy or their civil rights and civil liberties.
- Provide legally required protections based on the individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.

6. The labels assigned to existing information (see Section E.5 above) will be reevaluated whenever:
   - New information is added that has an impact on access limitations or the sensitivity of disclosure of the information.
   - There is a known change in the use of the information affecting access or disclosure limitations; for example, the information becomes part of court proceedings for which there are different public access laws, i.e. Freedom of Information Act (FOIA).

7. NVRIC 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. NVRIC personnel will:
   - Prior to allowing access to or dissemination of the information, ensure that attempts to validate or refute the information have taken place and that the information has been assessed for sensitivity and confidence by subjecting it to an evaluation or screening process to determine its credibility and value and categorize the information as unsubstantiated or uncorroborated if attempts to validate or determine the reliability of the information have been unsuccessful. The center will use a standard reporting format.
   - Store the information using the same storage method used for data that rises to the level of reasonable suspicion and which includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information.
   - Allow access to or disseminate the information using the same (or a more restrictive) access or dissemination standard that is used for data that rises to the level of reasonable suspicion (for example, "need-to-know" and "right-to-know" access or dissemination for personally identifiable information).
   - Regularly provide access to or disseminate the information in response to an interagency inquiry for law enforcement, homeland security, or public safety and analytical purposes or provide an assessment of the information to any agency, entity, individual, or the public when credible information indicates potential imminent danger to life or property.
   - Retain information for up to three years in order to work an unvalidated tip, lead, or SAR information to determine its credibility and value or assign a

"disposition" label (for example, undetermined or unresolved, cleared or unfounded, verified, or under active investigation) so that a subsequently authorized user knows the status and purpose for the retention and will retain the information based on the retention period associated with the disposition label.

- Adhere to and follow the center's physical, administrative, and technical security measures to ensure the protection and security of tips, leads, and SAR information. Tips, leads and SAR information will be secured in a system that is the same as or similar to the system that secures data that rises to the level of reasonable suspicion.

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

9. The NVRIC 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 labels, which will enable ISE authorized users to determine the nature of the protected information and how to handle the information in accordance with applicable legal requirements.

10. The NVRIC requires certain basic descriptive information (metadata tags or labels) to be entered and electronically associated with data (or content) for which there are special laws, rules, or policies regarding access, use, and disclosure, including terrorism-related information shared through the ISE. The types of information include:
    - The name of the originating center, department or agency, component, and subcomponent.
    - The name of the center's justice information system from which the information is disseminated.
    - The date the information was collected and, when feasible, the date its accuracy was last verified.
    - The title and contact information for the person to whom questions regarding the information should be directed.

11. The Northern Virginia Regional Intelligence Center will attach 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.

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

F. Acquiring and Receiving Information

1. Information gathering (acquisition) and access and investigative techniques used by the NVRIC and information-originating agencies will remain in compliance with and will adhere to applicable law and guidance, including, but not limited to:
    - 28 Code of Federal Regulations (CFR) Part 23 regarding criminal intelligence information.
    - The Fair Information Practice Principles (FIPPs); see Appendix A, "Fair Information Practice Principles", but not that under certain circumstances, the FIPPs may be superseded by authorities paralleling those provided in the federal Privacy Act; state, local, tribal, or territorial law; or center policy).
    - Criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) *National Criminal Intelligence Sharing Plan* (NCISP) (Ver. 2).
    - Constitutional provisions and administrative rules identified in Appendix B, as well as regulations and policies that apply to multijurisdictional intelligence and information databases and participating agency regulations.

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

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

4. Information gathering and investigative techniques used by the NVRIC, and participating agencies 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.

5. External agencies that access the NVRIC'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.

6. The NVRIC 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.

7. The NVRIC 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.

G. Information Quality Assurance

1. The NVRIC will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources; 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 as found in Section I - Merging Records, has been met.

2. The NVRIC will put in place a process for additional fact development during the vetting process where a SAR includes PII and is based on behaviors that are not inherently criminal. The NVRIC will articulate additional facts or circumstances to support the determination that the behavior observed is not innocent but rather reasonably indicative of preoperational planning associated with terrorism.

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

4. The NVRIC makes notification, in a timely manner, alleged errors and deficiencies (or refers them to the originating agency). The NVRIC corrects,

deletes, or refrains from using protected information found to be erroneous or deficient.

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

6. The NVRIC 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).

7. Originating agencies external to the NVRIC 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.

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

H. Collation and Analysis

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

2. Information subject to collation and analysis is information as defined and identified in Section E.

3. Information acquired or received by the Northern Virginia Regional Intelligence Center 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.

4. The NVRIC requires that all analytical products be reviewed and approved by the Privacy Officer, and the Director, Deputy Director, Operations Manager or his/her designee, to ensure that they provide appropriate privacy, civil rights, and civil liberties protections prior to dissemination or sharing by the center.

I. Merging Records

1. Information will be merged only by qualified individuals who have successfully completed a background check and possess the appropriate security clearance, if applicable, and have been selected, approved, and trained accordingly.

2. Records about an individual or organization from two or more sources will not be merged by the Northern Virginia Regional Intelligence Center 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.

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

J. Sharing and Disclosure

1. Credentialed, role-based access criteria will be used by the NVRIC, 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.

1. Access to or disclosure of records retained by the NVRIC can be provided only to persons within the center or in other governmental agencies whom 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.

2. To the extent possible, the NVRIC will not authorize any agency external to the center to disseminate information accessed or disseminated from the center without approval from the center and the originator of the information.

3. Records retained by the NVRIC may be accessed by or disseminated to those responsible for public protection, public safety, or public health only for public protection, public safety, public health purposes or specific 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.

4. Information gathered or collected and records retained by the NVRIC 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.

5. The NVRIC shall not release any information to any person or agency that would not be eligible to receive the information unless 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.

6. The Northern Virginia Regional Intelligence Center adheres to the current version of the ISE-SAR Functional Standard for its suspicious activity reporting (SAR) process, including the use of a standard reporting format and commonly

accepted data collection codes and a sharing process that complies with the ISE-SAR Functional Standard for suspicious activity potentially related to terrorism.

7. Information gathered or collected and records retained by the Northern Virginia Regional Intelligence Center 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 three years by the center.

8. 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 § 19.2-389 Code of Virginia.
    - 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.
    - Investigatory records (criminal investigative file documents and information and other records) of law enforcement agencies that are exempted from disclosure requirements under § 2.2-3706 Code of Virginia.
    - 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 § 2.2-3705.2 Code of Virginia. This includes a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism, including 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 applicable law, be shared without permission.

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

K. Redress

1. The NVRIC will follow the redress procedures below when a complaint involves records that have or have not been disclosed to the complainant under applicable law.
    - If an individual has complaints or objections to the accuracy or completeness of information and intelligence gathered and records retained by the NVRIC about him or her that is alleged to be held by the NVRIC, the NVRIC, as appropriate, will inform the individual of the procedure for submitting requests for information or complaints and requests for corrections to information and the resulting action in response to such requests, if any. The request will he handled through the Fairfax County Police Department, Internal Affairs Bureau, Inspections Division, which can sent to 12099 Government Center Parkway, Fairfax, VA 22035.
    - The NVRIC will acknowledge complaints regarding information that is exempt from disclosure and state that it will be reviewed but will not confirm the existence of any information and intelligence gathered and records retained by the NVRIC that identifies the individual. However, any personal information will be reviewed and corrected in or deleted from any NVRIC database if the information is determined to be erroneous, include incorrectly merged information, or to be out of date.
    - A record will be kept of all requests and of what information is disclosed to the individual.

2. The existence, content, and source of the information will not be made available by the NVRIC to an individual when information is exempt from disclosure by law and:
    - 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 system subject to 28 CFR Part 23 [see 28 CFR § 23.20(e)].
    - The center did not originate and does not have a right to disclose the information.

3. 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.

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

5. 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 NVRIC or the originating agency. The individual will also be informed of the procedure for appeal when the center or originating agency has cited an exemption for the type of information requested or has declined to correct challenged information to the satisfaction of the individual to whom the information relates.

6. If an individual has a complaint with regard to the accuracy or completeness of terrorism-related protected information that:
    - Is exempt from disclosure, and
    - Has been or may be shared through the ISE, and
    - Is held by the NVRIC, and
    - Allegedly has resulted in demonstrable harm to the complainant, then:
        - 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: Fairfax County Police Department, NVRIC Privacy Officer, 12099 Government Center Parkway, Fairfax, Virginia 22035.
        - The Privacy Officer or individual designated by the Director will acknowledge the complaint and state that it will be reviewed but will not confirm the existence or nonexistence of the information for 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 15 days and, upon request, assist such agency to correct any identified data/record deficiencies, purge the information, or verify that the record is accurate.
        - This request will then be sent to the Fairfax County Police Department, Internal Affairs Bureau, Inspections Division for review and if necessary, response.
        - 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, 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.

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

L. Security Safeguards

1. The NVRIC's Security Officer is designated and trained to serve as the center's security officer.

2. The NVRIC will comply with generally accepted industry or other applicable standards for security, in accordance with the NVRIC Dissemination Policy and Secure Room Policy. Security safeguards will cover any type of medium (printed and electronic) or technology (e.g. physical servers, virtual machines, and mobile devices) used in a work-related NVRIC activity.

3. The NVRIC operates in a secure facility protected from external intrusion. The center utilizes secure internal and external safeguards against network intrusions. Access to the center's databases from outside the facility will be allowed only over secure networks.

4. The NVRIC secures tips, leads, and SAR information in a separate repository system using security procedures and policies that are the same as or similar to those used for a system that secures data rising to the level of reasonable suspicion.

5. The NVRIC 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.

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

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

8. The NVRIC utilizes electronic audit trail watch logs to maintain audit trails of requested and disseminated information.

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

10. The NVRIC will, where applicable, notify an individual about whom personal information was or is reasonably believed to be breached or obtained by an unauthorized person and access to which threatens the physical, reputation, or financial harm to the person. Any notice will be made promptly and without unreasonable delay following the 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.

M. Information Retention and Destruction

1. All applicable information will be reviewed for record retention (validation or purge) by NVRIC at least every 3 years, as provided by 28 CFR Part 23.

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

3. The NVRIC 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.

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

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

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

N. Accountability and Enforcement

1. The NVRIC's Privacy Officer is responsible for receiving 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 the following address: Fairfax County Police Department, NVRIC Privacy Officer, 12099 Government Center Parkway, Fairfax, Virginia 22035. Depending on the inquirer and/or complaint, the query will then be sent to the Fairfax County Police Department's Internal Affairs Bureau, Inspections Division or the Fairfax County Attorney for response.

2. The NVRIC's trained Privacy Officer, will review and update the provisions protecting privacy, civil rights, and civil liberties contained in this policy annually and will make appropriate changes in response to changes in applicable law, technology, the purpose and use of the information systems, and public expectations.

3. The NVRIC 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.

4. The NVRIC will be open with the public in regard to information and intelligence collection practices. The center's privacy policy is available upon request and posted on the National Fusion Center Association website at www.new.nfcausa.org.

5. The audit log of queries made in Fairfax County's Record Management System will identify the user initiating the query.

6. The NVRIC maintains an audit trail of accessed, requested, or disseminated information. An audit trail is kept for a minimum of three years of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.

7. The NVRIC has adopted and follows 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 includes logging access to these systems and periodic auditing of these systems, so as to not establish a pattern of the audits. These audits are mandated at least annually and a record of the audits are maintained by the center.

8. The NVRIC's personnel or other authorized users shall report errors and suspected or confirmed violations of center policies relating to protected information to the center's Privacy Officer or the Director's designee.

9. The NVRIC will annually conduct an audit and inspection of the information and intelligence contained in its information system. The audit will be conducted by the Privacy Officer. The center's Advisory Board has the option of requesting and participating in 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).

10. If center personnel, a participating agency, or an authorized user is found to be in noncompliance with the provisions of this policy regarding the gathering, collection, use, retention, destruction, sharing, classification, or disclosure of information, the Director of the NVRIC, as appropriate will:
    - Suspend or discontinue access to information by the center personnel, the participating agency, or the authorized user.
    - Suspend, demote, transfer, or terminate center personnel, as permitted by applicable personnel policies.
    - Apply administrative actions or sanctions as provided by the NVRIC rules and regulations or as provided in agency/center personnel policies.
    - If the authorized user is from an agency external to the agency/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.
    - Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.
    - The NVRIC 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/Civil Rights Civil Liberties policy.

O. Training

1. The NVRIC requires all assigned personnel of the center or other individuals who have access to personal information, protected information, or other sensitive center data to participate in training programs regarding implementation of and adherence to the privacy, civil rights, and civil liberties policy.

2. The NVRIC provides 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.

3. The NVRIC's privacy/civil rights civil liberties policy training program covers:
    - 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.
    - Updates to the Privacy/Civil Rights Civil Liberties policy, if any, in response to changes in law and implementation experience
    - ISE Core Awareness Training, available at ise.gov
    - The nature and possible penalties for policy violations, including possible transfers, dismissal, criminal liability, and immunity, if any.

Appendix A: Terms and Definitions

28 CFR Part 23 — Section 28 Part 23 of the Code of Federal Regulations (CFR). This code governs Criminal Intelligence systems which receive federal funding to operate.

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

Acquisition — The means by which an Information Sharing Environment 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 Information Sharing Environment participants through, for example, news reports or to the obtaining of information shared with them by another Information Sharing Environment participant who originally acquired the information.

Agency — The Fairfax County Police Department and all agencies that access, contribute, and share information in the Fairfax County Police Department'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.

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

Center — Refers to the Northern Virginia Regional Intelligence Center.

Civil Liberties — Fundamental individual rights granted, 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.

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.

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.

Fair Information Practice Principles — The Fair Information Practice Principles (FIPPs) are contained within the Organization for Economic Co-operation and Development's (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. These were developed around commercial transactions and the transborder exchange of information; however, they do provide a straightforward

description of underlying privacy and information exchange principles and provide a simple framework for the legal analysis that needs to be done with regard to privacy in integrated justice systems. Some of the individual principles may not apply in all instances of an integrated justice system.

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

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.

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).

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 Information Sharing Environment, 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 counterintelligence investigation, assessment of or response to criminal threats and vulnerabilities, the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of or response to criminal acts and violations of the law, identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance.

Logs — 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.

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.

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.

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

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

Protected Information — Protected information includes Personal Data about individuals 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; Virginia state constitution; and applicable state and local laws, ordinances, and codes or the provisions of this 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 a participating agency.

Public does not include:

- Employees of the center or a 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.

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.

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 Information Sharing Environment-Suspicious Activity Report 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 or sensitive infrastructure facilities, site breach or physical instruction, 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 Information Sharing Environment 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 Information Sharing Environment will facilitate the sharing of "terrorism information," as defined in the IRTPA, as well as the following categories of information to the extent that they do not otherwise constitute "terrorism information": (1) homeland security information as defined in Section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. § 482(f)(1); and (2) law enforcement information relating to terrorism or the security of our homeland). Such additional information may include intelligence information.

Tips and Leads Information or Data — 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 suspicious.

A tip or lead can come from a variety of source, 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: Laws and Regulations Governing Privacy-Information Sharing

Federal

The United States Constitution
Title 18, United State Code (USC), Section 641 – Theft of Government Property
- 18 USC 1020 – Fraud and related activity in connection with computers
- 18 USC 1343 – False Pretense or misrepresentation
- 18 USC 1951 – Misuse of public office duties and responsibilities (Hobbs Act)
- 18 USC 1952 – Promote or carry on any unlawful activity

Title 28 Code of Federal Regulations, Part 23
The Privacy Act of 1974 – United States Code Section 552a as Amended
USA PATRIOT Act, Public Law No. 107-56 (October 26, 2001), 115 Stat. 272

State

The Constitution of Virginia
The following Virginia Code Sections:

§ 2.2 – 3706	Disclosure of Criminal records limitations
§ 2.2 – 3800	Government Data Collection and Dissemination Practices Act
§ 2.2 – 3801	Definitions
§ 2.2 – 3802	Systems to which chapter inapplicable
§ 2.2 – 3803	Administration of systems including personal information; Internet privacy policy; exceptions
§ 2.2 – 3805	Dissemination of reports
§ 2.2 – 3806	Rights of data subjects
§ 2.2 – 3807	Agencies to report concerning systems operated or developed; publication of information
§ 18.2 – 152.4	Computer Trespass
§ 18.2 – 152.5	Computer Invasion of Privacy
§ 18.2 – 152.7	Personal trespass by computer
§ 19.2 – 389	Dissemination of criminal history record information

Departmental Directives

Fairfax County Police Department General Order 204 – Administrative Activities
Fairfax County Police Department Standard Operating Procedure 07-032 Officer Safety Alerts