Virgin Islands Fusion Center

Privacy Policy

Reviewed 1/12/2014

The mission of the Virgin Islands Fusion Center is to prevent and deter acts of terrorism and criminal activity within the territory of the U.S. Virgin Islands, and to promote public safety through intelligence fusion and information sharing with all its law enforcement partners.

1.0 PURPOSE STATEMENT

The Virgin Islands Analysis and Information Center (VIFC) is established to provide the information sharing and exchange of terrorism and crime-related information among members of the law enforcement community while following the Fair Information Practices to ensure the rights and privacy of citizens. The focus of the VIFC is to combine the intelligence and information sharing efforts of all participating agencies to enhance the ability to predict, prevent, and respond to unlawful activity and threats to our nation. This is a process whereby information is collected, integrated, evaluated, analyzed and disseminated through established procedures for law enforcement purposes and in the interest of public safety. The intelligence products and services are made available to law enforcement agencies and other entities contributing to public safety throughout the VIFC and the country. The VIFC recognizes the importance of this privacy policy throughout the intelligence process in order to promote

1. Increasing public safety and improving national security.
2. Minimizing the threat of and risk of injury to specific individuals.
3. Minimizing the threat and risk of injury to law enforcement and others responsible for public protection, safety, or health.
4. Minimizing the threat and risk of damage to real or personal property.
5. Protecting individual privacy, civil rights, civil liberties, and other protected interest
6. Protecting the integrity of the criminal investigatory, criminal intelligence and justice system processes and information.
7. Minimizing the reluctance of individuals or groups to cooperate with the justice system.
8. Making the most effective use of public resources allocated to public safety agencies.

2.0 COMPLIANCE WITH LAWS REGARDING PRIVACY, CIVIL LIBERTIES AND CIVIL RIGHTS

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

The VIFC will provide a printed copy of this policy to all center and non center 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. Additionally a hard copy of this policy will be available at the center at all times for review.

All VIFC personnel, participating agency personnel providing information technology services to the center, private contractors, agencies that originate information and other authorized users are in compliance with applicable laws protecting privacy, civil rights and civil liberties including but not limited to:

- US Patriot Act, Public Law No. 107-56 (October 26,2001) 115 Stat 272
- 28 CFR Part 23
- U.S. Constitution, First, Fourth and Sixth Amendments
- Federal Records Act, 15 U.S.C § 3301, United States Code, Title 44, Chapter 33 § 3301
- Criminal Justice Information Systems, 28 CFR Part 20, Code of Federal Regulations Title 28, Chapter 1, Part 20
- Crime Identification Technology, 42 U.S.C § 14601, United States Code, Title 42, Chapter 140, Subchapter l, § 14601

The VIFC has adopted internal operating policies that are in compliance with applicable laws protecting privacy civil rights and civil liberties including but not limited to,

- US Patriot Act, Public Law No. 107-56 (October 26,2001) 115 Stat 272
- 28 CFR Part 23
- U.S. Constitution, First, Fourth and Sixth Amendments
- Federal Records Act, 15 U.S.C § 3301,United States Code, Title 44, Chapter 33 § 3301
- Criminal Justice Information Systems, 28 CFR Part 20, Code of Federal Regulations Title 28, Chapter 1, Part 20
- Crime Identification Technology, 42 U.S.C § 14601, United States Code, Title 42, Chapter 140, Subchapter l, § 14601
- Title 10 V.I.C Civil Rights Act
- Title 3 V.I.C Chapter 33 Public Records Act
- 3 V.I.C 881 Public right to access public records
- 23 V.I.C. 1032 Homeland Security Act, regarding intelligence information
- The Organic Act §34 Bill of Rights and Restrictions

The Director of the center oversees the daily operation of the center as well as having the responsibility for the operation of its justice systems, operations, coordination of personnel. Additional responsibilities include the receiving, seeking, retention, evaluation, information quality, analysis destruction, sharing or disclosure of information. The enforcement of this policy is assigned to VIFC security/privacy officer.

The Center is guided by a Board of Directors that is designated as a privacy committee that liaises with community privacy advocacy groups to ensure that privacy and civil rights are protected within the provisions of this policy and collection, retention and dissemination processes and procedures. In addition, the committee

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.

The fusion center privacy committee is guided by a trained privacy officer, whose primary responsibility is as the fusion center's security officer. The position which is appointed by the Director of the fusion center, oversees the implementation of privacy protections, ensures that the center adheres to the provisions of the ISE Privacy Guidelines, and receives and coordinates complaint resolution under the centers redress policy. The privacy officer can be contacted at the following address:

VITEMA Headquarters
Virgin Islands Fusion Center
Attn. Privacy Officer
1A & 1B Nisky
St. Thomas VI 00802

The VIFC Privacy Officer ensures the enforcement procedures and sanctions as outlined in Section 13.0 Accountability, within this policy are adequate and enforced.

3.0 DEFINITIONS

Appendix A provides definitions for words or phrases contained in this policy

4.0 INFORMATION COLLECTION

Each participating agency will determine which database(s) it will provide, and access to such databases will be governed by the laws that govern the particular agency respecting such data as well as applicable federal laws and in compliance of Code of Federal Regulations (28 CFR part 23).

Because the laws governing information that can be sought, collected or released on private individuals will vary from agency to agency, limitations on the collection of data concerning individuals is the responsibility of the collector of the original source data. Each contributor of information will abide by the collection limitations applicable to it by reason of law. Information contributed to the Virgin Islands Fusion Center should be that which has been collected in conformance with those limitations.

The following provisions set out the policies that will guide the operation of the Virgin Islands Fusion Center in four areas: 1) the types of information that may be sought and the types of information that may be collected or retained; 2) information that may not be sought, collected, or retained; 3) permissible methods of seeking information, including the receipt of information from third parties in the form of unsolicited tips; and 4) assessing information with respect to its validity, reliability, and access or disclosure.

4.1 Information That May Be Sought or Retained

The VIFC will seek or retain information only under the following circumstances:

1. The source of the information is reliable and verifiable.
2. Information supports reasonable suspicion the individual or organization is involved in criminal conduct, and the information is relevant to that conduct.
3. Information was collected in a fair and lawful manner, with knowledge and consent of the individual, if appropriate.
4. The information is relevant to the investigation and prosecution of terrorist and criminal acts or activity.
5. The information is useful in crime analysis or in the administration of criminal justice and public safety to include topical searches.
6. The information is based on a possible threat to public safety or the enforcement of criminal law.
7. Where there is reasonable suspicion that a specific individual or organization has committed a criminal offense or is involved in or is planning terrorist or criminal acts that presents a threat to a community, individual, or nation and the information is relevant to the act or activity.
8. Information may not be collected by VIFC or information-originating agencies will agree not to submit information about individuals solely on the basis of their political, religious or social views or activities, race, ethnicity, citizenship, place of origin, age, disability, gender, sexual orientation, participation in a particular noncriminal organization or lawful event, associations, or activities of any individual, group, or organization unless the information directly relates to criminal conduct or activity, and there is a basis of reasonable suspicion that the subject is involved in the illegal conduct.

The VIFC will abide by daily operating procedures for the initial collection and verification of intelligence, including the screening process by an analyst/call taker and Subsequent review by supervisory personnel.

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 in this policy.

The VIFC is maintained for the purpose of developing information and intelligence for and by participating stakeholder agencies. The decision of the agencies to participate with the fusion center and to decide which databases to provide for fusion center access is voluntary and will be governed by the laws and rules governing those individual agencies, as well as by applicable federal laws.

The center applies labels to agency oriented information (or ensures that the originating agency has applied labels) to indicate to the authorized user that:

- The information is “Protected Information” to include “personal data” (see Appendix A) on any individuals regardless of citizenship or U.S. residency status and to the extent expressly provided in this policy. Includes organizational entities.

- The information is subject to state and federal laws restricting access use or disclosure (i.e. the identity of a sexual assault victim or a minor).

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

- The information consists of tips and leads data, suspicious activity reports, criminal intelligence information, case records etc.
- Nature of the source as it affects veracity (examples: anonymous tip, trained interviewer or investigator public record or private sector.)
- Reliability of the source categorized as reliable, usually reliable, unreliable and unknown.
- Validity of the content (confirmed, probable, doubtful, cannot be judged).

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

- Protect confidential sources and police undercover techniques and methods.
- Not interfere with or compromise pending criminal investigations.
- Protect individual's right of privacy or his or her civil rights and liberties.
- Provide legally required protections based on the individuals 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.

The labels assigned to existing information under Section 4.1 will be reevaluated whenever:

- New information is added that has an impact on access limitations on the sensitivity of disclosure of the information.
- There is a change in the use of the information affecting access or disclosure limitations; for example, the information become part of court proceedings for which there are different public access laws.

Center 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. Center 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 the information has been assessed for sensitivity and confidence by subjecting it to and evaluation process to determine its credibility and value and categorize the information as unsubstantiated or uncorroborated if attempts to validate or determine the validity of the

information has been unsuccessful. The center will use a standard reporting format and data collection codes for SAR information.

- Store the information using the same storage method used for data that rises to the level of reasonable suspicion and includes an audit and inspection process, supporting documentation, and labeling of the information to delineate it from other information.

- Allow access to or disseminate the information using the same or more restrictive access or dissemination standard that is used that is used for data that rises to the level of reasonable suspicion.

- 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 five years to investigate an invalidated tip or lead or SAR to determine its credibility and value or assign a disposition label so that a subsequently authorized user knows that status and purpose of 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 or similar to the system that secures data that rises to the level of reasonable suspicion.

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

The VIFC 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 mechanism, including but not limited to metadata or data field labels that will enable ISE authorized users to determine the nature of the protected information and hoe to handle the information in accordance with applicable legal requirements.

The center requires certain basic descriptive information to be entered and electronically associated with data for which there are special laws, rules or policies regarding access, use and disclosure, including terrorism related information shared through the Information Sharing Environment.

The types of information should include:

- The name of the originating department, component and subcomponent.

- The name of the agency's justice information system from which the information was disseminated.

- The date the information was collected and where feasible, the date its accuracy was last verified.
- The title and contact information for the person requesting the information should be directed.

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

The center will keep a record of the source of all information sought and retained by the agency.

Information gathering and investigative techniques used by the center and information originating agencies are in compliance with and will adhere to applicable regulations and guidelines including but not limited to: 28 CFR Part 23, regarding criminal intelligence information.

- Organization for Economic Co-operation and Development (OECD) Fair Information Practices.
- Applicable criminal intelligence established under the U.S. Department of Justice's (DOJ) National Criminal Intelligence Sharing Plan (NCISP).
- Applicable constitutional provisions, Virgin Islands laws (including those referenced in Section 2.0), as well as any other regulations as reviewed by the Virgin Islands Office of the Attorney General that apply to multijurisdictional intelligence databases.

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

The 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 be documented and shared through the ISE. These safeguards are intended to ensure the information that could violate civil rights and civil liberties will not be intentionally gathered, documented, processed and shared.

Information gathering and investigative techniques used by the center will (and for originating agencies should) be the least intrusive means necessary in the particular circumstances to gather information it is authorized to seek or retain.

External agencies that access and share information with the center, are governed by laws and rules governing those individual agencies as by applicable federal and Virgin Islands laws.

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

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

- An individual or non governmental entity who may or may not receive a benefit or fee for providing information; or
- An individual or information provider that is legally prohibited from obtaining or disclosing information.

5.0 DATA QUALITY

The agencies participating in VIFC remain the owners of the data contributed and are, therefore, responsible for the quality and accuracy of the data accessed by the VIFC. Inaccurate personal information can have a damaging impact on the person concerned and on the integrity and functional value of the Center.

To ensure the accuracy of information received through database searches by cross-checks with other data systems and open source information and to maintain the integrity of the fusion center, any information obtained through the fusion center will be independently verified with the original source from which the data was extrapolated before any official action (e.g., warrant or arrest) is taken. User agencies and individual users are responsible for compliance with respect to use and further dissemination of such information and the purging and updating of the data. The VIFC will make every reasonable effort to ensure that information that is 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 stated in Section 6.0 Merging Records) has been met.

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

At the time of retention in the system the information will be labeled regarding its level of quality (accurate, complete, current, verifiable and reliable). The center also investigates in a timely manner alleged errors and deficiencies (or refers them back to the originating agency) and corrects, deletes or refrains from using protected information found to be erroneous or deficient.

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

VIFC will conduct periodic data quality reviews of information it originates and in the event the center learns that information gathered is erroneous, false or misleading, out of date, cannot be verified or is otherwise unreliable, the center did not have the authority to gather the information or to provide the information to any other agency, or the center used prohibited means to gather the information (except when the center's information source did not act as an agency of the center in gathering the information), the center will make every reasonable effort to ensure the data is corrected, not used by the center or to be completely deleted from the system.

When information supplied to external agencies is found to be erroneous, out of date, unverifiable or otherwise unusable the center will use written or electronic notification or both to notify recipients of such information has been deleted or changed by the center.

6.0 MERGING RECORDS

Records about an individual, group or organization from two or more sources will not merged unless there is sufficient information to reasonably conclude that the information is about the same individual, group or organization. Examples of information sufficient to allow merging include name full or partial, date of birth, fingerprints, telephone number, address, and tax ID number.

If there is an incomplete matching but there may be a partial match the data may be associated if a clear statement that complete matching has not been adequately established that the information relates to the same individual, group or organization.

7.0 USE LIMITATION

Information obtained from or through the VIFC can only be used for lawful purposes. A lawful purpose means the request for data can be directly linked to a law enforcement agency's active criminal investigation, or is a response to confirmed information that requires intervention to prevent a criminal act or threat to public safety.

Credentialed, role-based access criteria will be used by VIFC, 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.

The VIFC adheres to the current version of the ISE-SAR Functional Standard for its 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.

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

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

Information gathered or collected and records retained by the VIFC may be accessed or disseminated **for specific purposes** upon request by persons 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 access 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 20 years by the center.

Agencies external to the Virgin Islands Fusion Center may not disseminate information accessed or disseminated from the fusion center without approval from the fusion center or other originator of the information.

The VIFC Director reserves the right to deny access to any fusion center user who fails to comply with the applicable restrictions and limitations of the fusion center policy.

8.0 SECURITY

The VIFC's watch commander is designated and trained to serve as the center's security officer.

The VIFC will take the necessary measures to ensure access to the fusion center's information and intelligence resources is secure. Unauthorized access or use of the resources is forbidden.

Information gathered or collected and records retained by the VIFC will **not be:**

- Sold, published or exchanged for commercial purposes.
- Disclosed or published without prior notification 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 center.
- Disseminated to persons not authorized to access or use the information.

All personnel having access to VIFC data agree to abide by the following rules:

1. The fusion center's data will be used only in support of official law enforcement activities.
2. Individual passwords will not be disclosed to any other person, except as authorized by VICF management.
3. Individual passwords of authorized personnel will be changed if the password is compromised or improperly disclosed.
4. Background checks will be completed on personnel who will have direct access to the fusion center.
5. Use of the fusion center's data in an unauthorized or illegal manner will subject the requestor to denial of further use of the fusion center; discipline by the requestors employing agency and/or criminal prosecution.

Research of VIFC's data sources are limited to those individuals who have been selected, approved, and trained accordingly. Access to information contained within the fusion center will be granted only to fully authorized personnel who have been screened with state and national finger print-based background checks, as well as any additional background standards established by the VIFC Board. Information subject to collation and analysis is information as defined in (Refer to lll, Information). Information acquired or received by the VIFC 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 or engaging in criminal (including terrorist activities)

The VIFC requires that all analytical products be reviewed (and approved) by the Privacy Officer to ensure they provide appropriate privacy, civil rights and civil liberties protections prior to dissemination by the center. The VIFC will secure 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 under 28 CFR Part 23.

The VIFC 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.

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

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

The VIFC Director will identify technical resources to establish a secure facility for fusion center operations with restricted electronic access, security cameras, and alarm systems to guard against external breach of the facility. In addition, the VIFC Director will identify technological support to develop secure internal and external safeguards against network intrusion of fusion center data systems. Access to the fusion center's databases from outside of the facility will only is allowed over secure network lines.

9.0 RETENTION, REVIEW, PURGE, AND DESTRUCTION OF INFORMATION

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

2. When information has no further value or meets the criteria for removal according to the Virgin Islands Fusion Center retention and destruction policy it will be purged, destroyed, and deleted or returned to the submitting (originating) agency.
3. The Virgin Islands Fusion Center 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 Virgin Islands fusion Center 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 Virgin Islands Fusion Center, 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 Virgin Islands Fusion Center, 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.

10.0 OPENNESS

It is the intent of the VIFC and participating agencies to be open with the public concerning data collection practices when such openness will not jeopardize ongoing criminal investigative activities. The Virgin Islands Fusion Center will refer citizens to the original collector of the data as the appropriate entity to address any concern about data accuracy and quality, when this can be done without compromising an active inquiry or investigation.

The VIFC will be open with the public in regard to information and intelligence collection practices. The center's privacy policy will be provided to the public for review, made available upon request, and posted on the center's website (site pending) .

The VIFC's Privacy Officer will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights and civil liberties protections in the information system(s) maintained or accessed by the center. The Privacy officer can be contacted at:

VITEMA Headquarters
Virgin Islands Fusion Center
Attn. Privacy Officer
1A & 1B Nisky
St. Thomas VI 00802

11.0 INDIVIDUAL PARTICIPATION

The data maintained by the VIFC is obtained through participating stakeholder agencies, federal agencies, and open source resources. Individual users of fusion center information are solely responsible for the interpretation, further dissemination, and use of information developed in the research process. Additionally, it is the responsibility of the user to ensure the accuracy, validity, and completeness of all intelligence information obtained prior to official action being taken in full or in part.

Information gathered or collected and records retained by the VIFC may be accessed or disclosed ***to a member of the public*** only if the information is defined by law to be a public record or otherwise appropriate for release to further the center's mission and is not exempt from disclosure by law. Such information may be disclosed only in accordance with the law and procedures applicable to the center for this type of information. An audit trail sufficient to allow the identification of each individual member of the public who accessed or received information retained by the center and the nature of the information accessed will be kept by the center. Members of the public cannot access personal information for themselves or others from the VIFC applications. Persons wishing to access personal data pertaining to themselves should communicate directly with the agency or entity responsible for the data in question. Upon request the VIFC may supply the name of the originating agency of the requested information. Participating agencies agree that they will refer requests related to privacy back to the originator of the information.

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 Virgin Island Fusion Center. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information (correction). The center's response to the request for information will be made within a reasonable time and in a form that is readily intelligible to the individual. A record will be kept of all requests and of what information is disclosed to an individual.

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 Title3 V.I.C. Chapter 33 Public Records Act.
- Information that meets the definition of "classified information" as the term is defined in the National Security Act, Public Law 235, Section 606, and in accordance with Executive Order 13549, Classified

National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010.

- Investigatory records of law enforcement agencies that are exempted from disclosure requirements under 33 V.I.C 881. However, certain law enforcement records must be available for inspection and copying under Title 3V.I.C. Chapter 33 Public Records Act.

- 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 under 23 V.I.C 1032. This includes a record assembled, prepared or maintained to prevent, mitigate or respond to an act of terrorism under Title 23 V.I.C. Subchapter II Homeland Security Act §1032 or an act of agricultural terrorism under Title 23 V.I.C. Subchapter II Homeland Security Act §1032 and PCII agreements vulnerability assessment, risk planning document, 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 3 V.I.C Chapter 33 Public Records Act specifically § 881 and Federal Records Act 15 U.S.C § 3301 be shared without permission.

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

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

- Disclosure would interfere with, compromise or delay an ongoing investigation or prosecution.3 V.I.C 881.

- Disclosure would endanger the health or safety of an individual, organization or community. Title 23V.I.C.Chapter 4.

- The information is in a criminal intelligence information system subject to 28 CFR §23.20(e).

- The information relates to 3 V.I.C. 881.

- The center did not originate and does not have a right to disclose the information.

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.

The VIFC 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.

Corrections:
If an individual requests correction of information originating with the VIFC that has been disclosed, the center's Privacy Officer or designee 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.

Appeals:
The individual who has requested disclose or to whom information has been disclosed will be given the reasons if disclose or requests for correction are denied by VIFC 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.

Complaints:
If an individual has a complaint with regard to the accuracy or completeness of terrorism-related protected information that:
(a) Is exempt from disclosure,
(b) Has been or may be shared through the ISE,
(1) Is held by the VIFC and
(2) Allegedly has resulted in demonstrable harm to the complainant, the center will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the center's Privacy Officer at the following address:

VITEMA Headquarters
Virgin Islands Fusion Center
Attn. Privacy Officer
1A & 1B Nisky
St. Thomas VI 00802

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 complaint unless otherwise required by law. If the information did not originate with the center, the Privacy Officer will notify the originating agency in writing or electronically within 10 days and upon request, assist such agency to correct any identified data/record deficiencies, purge the information, or verify that the record is accurate.

All information held by the center that is the subject of a complaint will be reviewed within 30 days and confirmed or corrected / purged if determined to be inaccurate or incomplete, to include incorrectly merged information or to be out of date. If there is no resolution within 30 days the center will not share the information until such time as the complaint has been resolved. A record will be kept by the center of all complaints and the resulting action taken in response to the complaint.

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

12.0 ACCOUNTABILITY

Queries made to the VIFC data applications will be logged into the fusion center's data system identifying the user initiating the query. When such information is disseminated outside of the originating agency, a secondary dissemination log will be created in order to capture updated information and provide an appropriate audit trail, as required by applicable law. Secondary dissemination of information can only be to a law enforcement agency for investigative purposes or to other agencies as provided by law. The agency from which the information is requested will maintain a record of any secondary dissemination of information. This record should reflect at a minimum:

1. Date of release.
2. The subject of the information
3. To whom the information was released (including address and telephone number).
4. An identification number or other indicator that clearly identifies the data released.
5. The purpose for which the information was requested.

VIFC will maintain an audit trail of accessed, requested or disseminated information. An audit trail will be kept for a minimum of 20 years of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.

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

The Board reserves the right to restrict the qualifications and number of personnel having access to the fusion center and to suspend or withhold service to any individual violating this Privacy Policy. The Board or persons acting on its behalf, further reserves the right to conduct inspections concerning the proper use and security of the information received from the fusion center.

The VIFC Governance Board with the concurrence of the Director of VITEMA will be responsible for conducting or coordinating random internal or special audits, and for investigating misuse of the fusion center's information systems. All confirmed or suspected violations of VIFC policies will be reported through the VIFC Director to the Director of VITEMA. Individual users of VIFC information remain responsible for the appropriate use of fusion center information. Each user of the fusion center and each participating agency within the VIFC are required to abide by this Privacy Policy in the use of information disseminated. Failure to

abide by the restrictions for the use of the VIFC data may result in the suspension or termination of user privileges; discipline imposed by the user's employing agency, or criminal prosecution.

13.0 TRAINING

All assigned personnel of the center, personnel providing information technology services to the center; staff in other public agencies or private contractors providing services to the center and users who are not employed by the center or a contractor will be required to participate in training programs regarding those regulations and implementation of and adherence to the privacy, civil rights, and civil liberties policy.

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

The VIFC's privacy policy training program will cover:

- Purposes of the privacy, civil rights and civil protections policy.
- Substance and intent of the provisions of the policy relating to the 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 system user.
- The impact of improper activities associated with infractions within or through the agency.
- Mechanisms for reporting violations of center privacy protection policies and procedures.
- The nature and possible penalties for policy violations including possible transfer, dismissal, criminal liability and immunity if any.

Appendix A.

"Board of Directors": The group of individuals charged with providing guidance for the operations of the VIFC to the Commissioner of Public Safety

“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 criminal intelligence system per 28 CFR Part 23.

"Executive Director": Head of the Executive Committee

“Director of the Virgin Islands Fusion Center”: Oversees the daily operations of the VIFC.

"Fusion center": The operations center consisting of analysts, watch officers, and other supervisors; synonymous with the VIFC

“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.

“**Personal Data”:** Refers to any information that relates to an identifiable individual (or data subject).

“Protected Information”: For the non intelligence community, protected information is information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and laws of the United States. While not within the definitions established by the ISE Privacy Guidelines, protections may be extended to other individuals and organizations by internal federal agency policy or regulation.

For the (federal) intelligence community, protected information includes information about “United States persons” as defined by Executive Order 12333. Protected information may also include other information that the U.S. government expressly determines by Executive Order, International agreement, or other similar instrument should be covered.

For the Virgin Islands, protected information includes Personal Data about individuals that is subject to information privacy or other legal protections by law, including the U.S. Constitution and the Virgin Islands constitution; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 23, and applicable Virgin Islands law. Protection may also be extended to organizations by VIFC policy.

"Reasonable Suspicion/Criminal Predicate": When sufficient facts are established to give a trained law enforcement officer or employee a basis to believe there is a reasonable possibility an individual or organization is involved in a definable criminal activity or enterprise. (28CFR Part 23)

"Requestor": The individual law enforcement officer or agency making a request for information from, or reporting an incident to, the VIFC; synonymous with "user." Also identifies an individual making a request for corrections.

"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.

"Stakeholder Agencies": Those agencies that will participate in the operations of the VIFC in addition to sharing and collecting information.

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

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

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

"Terrorism-Related Information": In accordance with the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended by the 9/11 Commission Act (August 3, 2007, P.L. 110-53), the ISE facilitates the sharing of terrorism and homeland security information, as defined in IRTPA Section 1016(a)(5) and the Homeland Security Act 892(f)(1) (6 U.S.C. § 482(f)(1)). See also *Information Sharing Environment Implementation Plan* (November 2006) and Presidential Guidelines 2 and 3 (the ISE will facilitate the sharing of "terrorism information," as defined in the IRTPA, as well as the following categories of information to the extent that they do not otherwise constitute "terrorism information": (1) homeland security information as defined in Section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. § 482(f)(1)); and (2) law enforcement information relating to terrorism or the security of our homeland). Such additional information may include

intelligence information.

"Tips and Leads Information or Data": Generally uncorroborated reports or information generated from inside or outside a law enforcement agency that allege or indicate some form of possible criminal activity. Tips and leads are sometimes referred to as suspicious incident report (SIR), suspicious activity report (SAR), and/or field interview report (FIR) information. However, SAR information should be viewed, at most, as a subcategory of tip or lead data. Tips and leads information does not include incidents that do not have a criminal offense attached or indicated, criminal history records, or CAD data. Tips and leads information should be maintained in a secure system, similar to data that rises to the level of reasonable suspicion. A tip or lead can come from a variety of sources, including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information may be based on mere suspicion or on a level of suspicion that is less than "reasonable suspicion" and, without further information or analysis, it is unknown whether the information is accurate or useful. Tips and leads information falls between being of little or no use to law enforcement and being extremely valuable depending on the availability of time and resources to determine its meaning.

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