TENNESSEE FUSION CENTER
PRIVACY POLICY

A. PURPOSE STATEMENT

The Tennessee Fusion Center (TFC) was established to provide timely information sharing and exchange of crime and terrorism-related information among members of the law enforcement community. The primary focus of the TFC is the development and dissemination of criminal and/or terrorist related information. 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 while providing appropriate privacy, civil rights and civil liberties safeguards. Thereby, intelligence products and services are made available to law enforcement agencies and other entities contributing to public safety throughout the state and country.

B. POLICY APPLICABILITY AND LEGAL COMPLIANCE

1. All TFC personnel, participating agency personnel, private contractors, and other authorized users will comply with the TFC privacy policy concerning the information the center collects, receives, maintains, archives, accesses or discloses to center personnel, government agencies, including agencies participating in the Information Sharing Environment (ISE), participating criminal justice and public safety agencies, as well as to private contractors and the general public.

2. The TFC will provide a printed copy of this policy to all agency and non-agency personnel who provide services and will require all personnel to sign a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and the provisions it contains.

3. Information gathering and collection and investigative techniques used by TFC personnel, participating agency personnel, private contractors, and other authorized users will comply with all applicable laws protecting privacy, civil rights, and civil liberties, including but not limited to
   A. The U.S. and Tennessee Constitutions

   B. Tennessee Public Records Act, Tenn. Code Ann. § 10-7-501, et seq.

   C. Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C. § 210, et seq.

   D. Family Educational Rights and Privacy Act of 1974 (FERPA), 20 U.S.C. § 1232(g)

E. Driver's Privacy Protection Act of 1994 (DPPA), 18 U.S.C. § 2721, et seq.

F. Uniform Motor Vehicle Records Disclosure Act, Tenn. Code Ann. § 55-25-101, et seq.

G. 28 CFR Part 23

H. The U.S. Department of Justice's (DOJ) National Criminal Intelligence Sharing Plan (NCISP)

4. The TFC has adopted internal operating policies that are in compliance with applicable law protecting privacy, civil rights, and civil liberties, including, but not limited to, the laws listed in section B.3.

C. GOVERNANCE AND OVERSIGHT

1. The Governance Board is the management body overseeing the direction of the TFC. TFC Directors, who oversee the day-to-day overall operational activities of the center, shall be the Tennessee Bureau of Investigation's Special Agent in Charge (SAC) of the Criminal Intelligence Unit (CIU) and the Tennessee Office of Homeland Security's Supervisory Intelligence Officer assigned to the TFC. TFC's primary operational responsibilities include the management of its Fusion systems, tactical and strategic intelligence analytical operations, coordination of personnel, receiving, seeking, retention, evaluations, information quality assurance, analysis, file deletion, sharing or disclosure of information and privacy policy enforcement. All of these responsibilities are assigned to the TFC's Directors.

2. The TFC recognizes the importance of ensuring the protection of individual constitutional rights, civil liberties, civil rights, and privacy interests throughout the intelligence process. In order to preserve these rights, TFC has created a Legal Working Group (LWG) and designated a trained Privacy Officer/s who will: ensure safeguards and sanctions are in place to protect personal information; receive reports regarding alleged errors and violations of this policy and coordinate complaint resolution; and serve as the liaison for the Information Sharing Environment (ISE), including ensuring that privacy protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy enhancing technologies. The LWG has developed, published, and created the following Privacy Policy and standards the TFC will adhere to for the collection, use, and security of information collected in the Consolidated Records Management System (CRMS) and in the Criminal Intelligence Management System (CIMS), as well as accountability guidelines for the management of such information. TFC Privacy Policy incorporates the principles of the Fair Information Practices as outlined by the National Criminal Justice Association (NCJA) and all applicable laws. The Privacy Officer may be

contacted at the following address: TFC Privacy Officer, TBI Professional Standards Unit, 901 R.S. Gass Boulevard, Nashville, TN 37216 and at TFC Privacy Officer, TDOS Legal Division, 1150 Foster Avenue, Nashville, TN 37243.

3. The Governance Board or its designee will take necessary measures to ensure that access to TFC's information and intelligence resources is secure. The Board reserves the right to restrict the qualifications and number of personnel having access to TFC and to suspend or withhold service to any individual or agency 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 TFC.

D. DEFINITIONS

1. C.F.R.: Code of Federal Regulations.

2. Consolidated Records Management System (CRMS): A database repository containing criminal incident/offense records, traffic related investigation/enforcement and other law enforcement activity records, submitted and updated by law enforcement agencies and criminal justice organizations into the CRMS, this includes additions, updates, or deletions of records as submitted by the originating agency. CRMS records are not Criminal Intelligence Information and as such, are not governed under 28 CFR Part 23.

3. Criminal Intelligence Management System (CIMS): The arrangements, equipment, facilities, and procedures used by TFC for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information.

4. Criminal Intelligence Information: Information compiled, analyzed and/or disseminated in an effort to anticipate, prevent, or monitor criminal or terrorist activity.

5. Fusion System: The composite of all technologies, both current and developed in the future, which support daily TFC operations, including, but not limited to the CRMS, CIMS and any other tools and technologies that allow TFC personnel to access law enforcement and criminal justice portals and open source databases.

6. Governance Board: The management body overseeing the direction of TFC.

7. Homeland Security Information: Any information possessed by a federal, state, local, or tribal agency that relates to (A) a threat of terrorist activity; (B) the ability to prevent, interdict, or disrupt terrorist activity; (C) the identification or investigation of a suspected terrorist or terrorist organization or any person, group, or entity associated with or assisting a suspected terrorist or terrorist

organization; or (D) a planned or actual response to a terrorist act. [Section 892(f) of the Homeland Security Act of 2002 (codified at 6 U.S.C. § 482(f)(1)].

8. Information Sharing Environment (ISE): The ISE is a trusted partnership among all levels of government in the United States, the private sector, and our foreign partners, in order to detect, prevent, disrupt, preempt, and mitigate the effects of criminal activity, including terrorism, against the territory, people, and interests of the United States by the effective and efficient sharing of criminal, terrorism and homeland security information.

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

10. Legal Working Group: A composite body of Tennessee Bureau of Investigation, Tennessee Department of Safety and Homeland Security, Tennessee Attorney General and United States Attorney's Office attorneys as well as TFC supervisory personnel, who provide Privacy Policy and overall fusion center related legal guidance and recommendations.

11. Levels of Access to TFC Information: See 17 - Stakeholder/Users.

12. 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

13. Operational Reference Information: Non-criminal intelligence information, gathered to inform and support law enforcement and criminal justice organizations critical field operations, investigations, special event and public safety planning, preparation and related duties and responsibilities.

14. Personal Data: Any information relating to an identifiable individual.

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

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

16. Privacy Officer/Custodian of the Records: The person designated by the Legal Working Group to oversee TFC's compliance with privacy laws and procedures as well as public records requests.

17. Reasonable Suspicion/Criminal Predicate: When sufficient facts and/or circumstances are established to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe there is a reasonable possibility an individual or organization is involved in a definable criminal activity, enterprise, or terrorism.

18. Requestor/User: The individual law enforcement officer or agency making a request for information from, or reporting an incident to the TFC.

19. 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.

20. Qualifications for Access:
    A. Each person having any level of access to the TFC, including, but not limited access to all TFC personnel, participating agency personnel, private contractors, and other authorized users, shall meet the following qualifications before gaining access to TFC:

        (1) Not have been convicted of or pleaded guilty to or entered a plea of nolo contendere to any felony charge;

        (2) Not have been convicted of or pleaded guilty to or entered a plea of nolo contendere to any charge which would require registration

as a sex offender under the law in any state, country, territory or other entity; and

(3) Have good moral character.

B. Each TFC participating agency shall be responsible for ensuring that anyone having access to TFC meets the above criteria.

21. **Stakeholder – Users**:

A. ***Fusion System Administrator*** - This person acts as the central point of contact (POC) and administrator for all Fusion System technology management issues and may also serve as the POC for the initial agency CRMS setup, addressing Agency Name, ORI and Administrator ID and Password setup for CRMS access. This person also develops training for agency administrators to ensure administrators are able to perform:

(1) Agency User Add, Change, Delete with proper level of access;

(2) User Password Reset;

(3) Agency User Training for Activity Query engine against CRMS;

(4) Agency User Training for WebRMS;

(5) Agency User Training for Data Element Filter;

(6) Agency User Training for Activity Audits; and

(7) Agency User Training for Emergency Incident Deletions.

B. ***Agency Administrator*** - This person acts as the central point of contact within an end point agency and performs administration for all agency CRMS/WebRMS users ID and Password setup as well as training on the proper use of the CRMS Activity Query and the appropriate components of the WebRMS. The Agency Administrator performs audits of the CRMS access to ensure proper use of the system. The Agency Administrator has access to and is properly trained in the use of the Activity Query and appropriate components of the WebRMS features of the CRMS. This person is typically the Records Administrator Contact for the agency

C. ***Agency User*** – This person has CRMS access to perform authorized queries against the Activity Repository, CRMS and can add, change, or delete records via the WebRMS product that are pertinent to their agency. These users are unable to alter records from another agency.

D. ***Investigator*** – This person has CRMS access to perform only queries against the Activity repository, CRMS or the WebRMS repository for their agency. These users are unable to alter any records in the system.

E. ***Test User*** - This user is active only in the test environment of the system and is not defined in the Production System.

22. Suspicious Activity Reports (SARs): 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.

23. Tennessee Fusion Center ("TFC"): The operations center consisting of analysts and supervisors. The Tennessee Fusion Center is a joint operation between the Tennessee Bureau of Investigation, created by the Tennessee Legislature under TCA 38-6-101 et seq, and the Office of Homeland Security, which was created by Governor Sundquist with Executive Order No. 36 (http://state.tn.us/sos/pub/execorders/sundquist%20executive%20order%20no.%2036.pdf) and renewed by Governor Bredesen with Executive Order No. 08 (http://state.tn.us/sos/pub/execorders/exec-orders-bred8.pdf), and transferred under the Department of Safety's purview by Governor Bredesen with Executive Order No. 48 (http://state.tn.us/sos/pub/execorders/exec-orders-bred48.pdf).

24. Terrorism Information: The existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism; Threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations; Communications of or by such groups or individuals; Groups or individuals reasonably believed to be assisting or associated with such groups or individuals; and includes weapons of mass destruction information. [Section 1016(a)(5), Intelligence Reform and Terrorism Prevention Act of 2004, as amended (IRTPA)(codified at 6 U.S.C. § 485(a)(5)]

25. Weapons Of Mass Destruction Information: Information that could reasonably be expected to assist in the development, proliferation, or use of a weapon of mass destruction (including a chemical, biological, radiological, or nuclear weapon) that could be used by a terrorist or a terrorist organization against the United States, including information about the location of any stockpile of nuclear

materials that could be exploited for use in such a weapon that could be used by a terrorist or a terrorist organization against the United States. [Section 1016(a)(6), Intelligence Reform and Terrorism Prevention Act of 2004, as amended (IRTPA)(codified at 6 U.S.C. § 485(a)(6)]

E. INFORMATION

1. The TFC is maintained for the purpose of developing information and criminal intelligence for and by participating stakeholder agencies, other law enforcement or government agency or other reliable sources. The decision of an agency to participate with or contribute to the TFC, as well as what information to provide for TFC access, is voluntary and will be governed by the laws and rules governing those individual agencies, as well as by applicable federal laws and regulations, including, but not limited to, the Federal Freedom of Information Act (FOIA), 5 U.S.C. § 552, and the Tennessee Public Records Act, Tenn. Code Ann. § 10-7-501.

2. The TFC will seek or retain information that it is legally permissible for the agency to seek or retain under the legal authorities of the TFC (see Definition of Tennessee Fusion Center at Section D. 23.) to seek or retain information, U.S. and Tennessee Constitutions, and the Tennessee Public Records Act, Tenn. Code Ann. § 10-7-501:

   A. Is based on a possible threat to public safety or the enforcement of the criminal law; or,

   B. 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,

   C. 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,

   D. Is useful in crime analysis or in the administration of criminal justice and public safety (including topical searches); and,

   E. The source of the information is reliable and verifiable or limitations on the quality of the information are identified; and,

F. 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.

3. The TFC will not seek or retain information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation. Information related to these factors may be retained if there is a reasonable relationship or relevance to such information and the effort to detect, anticipate, or prevent criminal activity and this information is not the sole basis for retention or indexing. When there is reasonable suspicion that a criminal relationship exists, the information concerning the criminal conduct or activity may be retained or indexed; however, it is the responsibility of the source agency or TFC personnel to ascertain and clearly affirm the relationship to the key element of criminal activity prior to the retention or indexing of the information.

4. The TFC will abide by its daily operating procedures for the initial collection and verification of criminal, homeland security or terrorist information, including the screening process by an analyst or call taker and the subsequent review by supervisory personnel.

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

   A. Whether the information is: operational reference data, criminal incident data, general data, tips and leads data, suspicious activity reports, or criminal intelligence information;

   B. The nature of the source (for example: anonymous tip, interview, public records, and private sector);

   C. The reliability of the source (for example: reliable, usually reliable, unreliable, unknown); and,

   D. The validity of the content (for example: confirmed, probable, doubtful, cannot be judged.)

6. The TFC requires certain basic descriptive information to be entered and electronically associated with data (or content) that is to be accessed, used, and disclosed, including:

A. The name of the originating department, source agency or other source providing the information;

B. The date the information was collected and to the extent possible, the date its accuracy was last verified;

C. The title and contact information for the person to whom questions regarding the information should be directed and who is accountable for the decision to submit the information and assuring it is believed to otherwise conform to TFC submission standards;

D. Any particular limitations to the use or disclosure of the information;

E. The nature of the source (for example, anonymous tip, interview, public records, private sector); and,

F. Labeling information for reliability and validity. Due diligence will be exercised by submitting Agency as well as TFC personnel in determining source reliability and content validity.

(1) Reliability

(a) Reliable – the source has been determined to be reliable

(b) Unreliable – the reliability of the source is doubtful or has been determined to be unreliable

(c) Unknown – the reliability of the source cannot be judged or had not as yet been assessed

(2) Validity

(a) Confirmed – the information has been corroborated by a trained law enforcement analyst or officer or other reliable source

(b) Doubtful – the information is of questionable credibility but cannot be discounted based on the knowledge and skills of the reviewer

(c) Cannot be judged – the information cannot be confirmed at the time of review

G. Unless otherwise indicated by the source or submitting agency, source reliability is deemed to be “unknown” and content validity “cannot be

judged." In such case, users must independently confirm source reliability and content validity with the source or submitting agency or through their own investigation.

H. TFC personnel may reject information as failing to meet any criteria for inclusion, and return such information to the submitting party with an indication of why it was rejected.

I. When information is retained, the date of review for such information, to determine whether it should be purged or continued to be retained will be noted (this can be done electronically via date stamping within the CIMS system).

7. The TFC applies labels to center-originated information (or ensures that the originating agency has applied labels) to indicate to the accessing authorized user that:

A. The information is protected information as defined by TFC to include personal information on any individual as provided herein and, to the extent expressly provided in this policy, includes organizational entities; and,

B. The information is subject to Tenn. Code Ann. § 10-7-501 et seq., laws restricting access, use, or disclosure.

8. When the decision is made to retain information, it will be labeled by record, data set or system or records pursuant to applicable limitations on access and sensitivity of disclosure in order to:

A. Protect confidential sources and police undercover techniques and methods;

B. Not interfere with or compromise pending criminal investigations;

C. Protect an individual's right of privacy and civil rights and civil liberties; and,

D. Provide legally required protection based on the individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.

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

A. New information is added that has an impact on access limitations or the sensitivity of disclosure of the information; or,

B. There is a change in the use of the information affecting access or disclosure limitations.

10. The TFC will identify and review protected information that is originated by the center prior to sharing that information in the ISE. The TFC will provide notice mechanisms, including but not limited to metadata or data fields that will enable ISE authorized users to determine the nature of the protected information and how to handle the information in accordance with applicable legal requirements.

11. The TFC requires certain basic descriptive information to be entered and electronically associated with data (or content) that is to be accessed, used, and disclosed, including:

    A. The name of the originating department, component and subcomponent;

    B. The name of the agency system from which the information is disseminated;

    C. The date the information was collected and the date its accuracy was last verified; and,

    D. The title and contact information for the person to who questions regarding the information should be directed.

12. The TFC will apply specific labels and descriptive metadata to information that will be accessed and disseminated to clearly indicate all legal restrictions on information sensitivity or classification.

13. The basic types of information collected by the TFC will include;

    A. Incident and Investigation Information: The TFC Fusion System will collect and retain criminal incident/offense reporting and records, enforcement related reporting or records, other law enforcement activity records such as supplemental investigative and other law enforcement information except criminal intelligence information. This information will be submitted by Law Enforcement Agencies and Criminal Justice Organizations, having been collected or obtained through the course of law enforcement or criminal justice organization response to a reported criminal incident or other official calls for service or investigation to include motor vehicle investigation and enforcement activities.

    B. Criminal Intelligence Information: Information compiled, analyzed and/or disseminated in an effort to anticipate, prevent, or monitor criminal activity.

(1) The TFC will adhere to Criminal Intelligence Systems Operating Policies Federal Regulation 28 CFR Part 23, as recommended within the National Criminal Intelligence Sharing Plan (NCISP). TFC personnel will endeavor to ensure information collected meets the following minimal guidelines:

(a) The source of the information is a participating stakeholder agency or other law enforcement or government agency or other reliable or validated source;

(b) Information, if accurate, supports reasonable suspicion that the individual or organization has committed, or is planning to commit criminal conduct or other potential threat to public safety, and the information is relevant to that conduct;

(c) Information is relevant to an active or ongoing investigation, field operational support activity, or prosecution of suspected criminal incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences by response of any such incident or response; or the prevention of crime reasonably believed likely to occur without such preventative effort or necessary to further a law enforcement or homeland security agencies ability to maintain public order and safety and protect life or property;

(d) Is such that the source of the information is reasonably believed to be reliable and is reasonably verifiable and, when appropriate, the limitations on the reliability or veracity of the information are clearly stated;

(e) Information accurately reflects what was reported by the participating stakeholder agencies, other law enforcement, government agency or other reliable source;

(f) Information was collected in a fair and lawful manner by the participating stakeholder agencies, other law enforcement or government agency or other reliable source;

(g) With knowledge and consent of the individual, if appropriate;

(h) Information that does not appear to meet the criteria set forth above shall be reviewed by a supervisor of the TFC for determination as to whether or not the information

should be collected by the TFC. Such review may include further investigation into the credibility of the information.

(i) The retention or classification of existing information will be reevaluated whenever; new information is added that has an impact on access limitations or the sensitivity of disclosure of the information; or there is a change in the use of the information affecting access or disclosure limitations; or information has been developed that suggests the existing information is no longer of intelligence or investigative value or otherwise no longer warrants retention.

(j) Records that are five years old and determined to no longer be active criminal intelligence information will be purged in accordance with approved TFC records retention schedules, with only statistical information being kept.

C. Tips and Leads / Suspicious Activity Reports: TFC will retain information that is based on mere suspicion, such as tips and leads, and/or Suspicious Activity Reports (SARs). This information will be retained within the CRMS - WebRMS in the original form as was received from contributing agency and in order to complete the required vetting, as outlined within Criminal Intelligence subsection, also entered into the CIMS system and as appropriate, contributed to the FBI eGuardian system. Tip and Leads received within the CRMS - WebRMS will be retained as uploaded by the originating agency for an indefinite period of time. Tips and leads or SARs that are moved into the CIMS will be retained for a period of five (5) years in order to work an unvalidated tip, lead, or SAR information to determine its credibility 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.

(1) TFC personnel will:

(a) Prior to allowing access to or dissemination of the information, assess it for sensitivity and confidence.

(b) Subject the information to an evaluation process to determine its credibility and value as well as categorize the information as unsubstantiated or uncorroborated, should attempts to validate or determine the reliability of the information fail.

(c) 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 date to delineate it from other information.

(d) Allow access to or disseminate the information using the same (or a more restrictive) access or dissemination method that is used for data that rises to the level of reasonable suspicion (for example, “need-to-know” and “right-to-know” access or dissemination.)

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

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

(g) TFC personnel will review the tip or lead SAR information for appropriateness of sharing the information with the FBI eGuardian system.

(h) TFC personnel will vet submitted SARs as set forth in the ISE-SAR functional standard, to determine whether the information qualifies as an ISE-SAR and contribution to the FBI eGuardian system.

(i) All validated ISE-SARs provided to the TFC, will be contributed to the FBI eGuardian system, unless the source agency requests otherwise.

(j) At such time as a decision is made to contribute SAR information to the FBI eGuardian system, TFC personnel will label it to the extent feasible, consistent with ISE-SAR functional standards and pursuant to applicable limitations on access and sensitivity of disclosure in order to:

(i) Protect an individual's right of privacy and civil rights and civil liberties;

(ii) Protect confidential sources and police undercover techniques and methods;

(iii) Not interfere with or compromise pending criminal investigations; and

(iv) Provide any legally required protection based on the individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.

(k) Adhere to and follow the center's physical, administrative, and technical security measures that are in place for the protection and security of tips and leads information.

(l) Tips, leads, and SARs will be initially retained within the CRMS. Upon the completion of the required vetting process, they may be entered into the CIMS.

(m) Routinely review information to determine if it should be purged.

(n) Tips/Leads/SARs determined to be unfounded will be purged from CIMS and, when it has been contributed to the FBI eGuardian system should also purged from the FBI eGuardian system.

(o) Incorporate 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.

D. Operational Reference Information: Subsequent to a specific request for information, the TFC will collect and retain Operational Reference Information, for the purpose of informing and supporting law enforcement and criminal justice organization's critical field operations, investigations, special event and public safety planning, preparations and related duties and responsibilities. Operational Reference Information will be clearly

marked as “Operational Reference Information Only – Non-Criminal Intelligence Information” and retained within a unique file, to be maintained within the TFC Fusion System, Consolidated Intelligence System or Patriarch. Operational Reference Information may be comprised of Open Source research data, details of current or previous law enforcement/criminal justice operational planning, maps, photographs, and other open record information, in order to serve as a historical reference and a continuing law enforcement knowledge base, related to incidents and events requiring unique or significant law enforcement operational support, situational or special event management, or public safety/public order operations and activities.

F. ACQUIRING AND RECEIVING INFORMATION

1. All of the TFC’s criminal intelligence, Tips and Leads/SARs and Operational Reference Information files meeting the standards of collection by the TFC, will comply with all internal operational policies, be retained in compliance when applicable with Title 28 CFR Part 23, and any applicable state or local statutes governing the collection, dissemination, retention, receipt, storage, maintenance, access, and destruction of information.

2. CRMS records comprise a database repository containing criminal incident/offense records, traffic related investigation/enforcement records or other law enforcement activity records, submitted and updated by law enforcement agencies and criminal justice organizations. The submitting agency controls and conducts all additions, updates, or deletions of records which were submitted by said originating agency. CRMS records are not Criminal Intelligence Information and as such, are not governed under 28 CFR Part 23, but are governed according to an executed Memorandum of Understanding and any laws or regulations which apply to the submitting agency.

3. All TFC personnel, participating agency personnel, private contractors, and other authorized users will comply with all applicable laws protecting privacy, civil rights, and civil liberties, including but not limited to:

   A. Tennessee Public Records Act, Tenn. Code Ann. § 10-7-501, et seq.

   B. Freedom of Information Act (FOIA), 5 U.S.C. § 552

   C. Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C. § 210, et seq.

   D. Family Educational Rights and Privacy Act of 1974 (FERPA), 20 U.S.C. § 1232(g)

   E. Driver's Privacy Protection Act of 1994 (DPPA), 18 U.S.C. § 2721, et seq.

F. Uniform Motor Vehicle Records Disclosure Act, Tenn. Code Ann. § 55-25-101, et seq.

4. The TFC'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 or terrorism 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.

5. The TFC's SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved in activities that have been determined to be consistent with criminal activities associated with terrorism will be documented and shared through the ISE. 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.

6. Information gathering and investigative techniques used by the TFC will be the least intrusive means necessary in the particular circumstance to gather information it is authorized to seek or retain.

7. The TFC will contract only with commercial database entities that provide an assurance that they gather personally identifiable information in compliance with local, state, tribal, territorial, and federal laws and which is not based on misleading information collection practices.

8. The TFC will not directly or indirectly receive, seek, accept, or retain information from: an individual or nongovernmental information provider who may or may not receive a fee or benefit for providing the information if the center knows or has reason to believe that the individual or information provider is legally prohibited from obtaining or disclosing the information, or that the source used prohibited means to gather the information.

G. INFORMATION QUALITY ASSURANCE

1. The TFC will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources of information. Such information should be accurate, current, and complete including the relevant context in which it was sought or received. Other related information that is merged with other information about the same individual or organization should be retained only when the applicable standard has been met.

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

3. The TFC investigates, in a timely manner, alleged errors and deficiencies and corrects, deletes or refrains from using protected information found to be erroneous or deficient.

4. The labeling of retained information will be reevaluated when new information is gathered that has an impact on the center's confidence, validity and reliability in retained information.

5. The TFC will conduct periodic data quality reviews of information it originates and will make every reasonable effort to ensure that information will be corrected, deleted from the system, or not used when the center learns that the information is erroneous, misleading, obsolete or otherwise unreliable.

6. Participating agencies, including agencies participating in the ISE, are responsible for the quality and accuracy of the data accessed by or shared with TFC. Originating agencies providing data remain the owners of the data contributed. TFC will advise the appropriate data owner, in writing if its data is suspected or found to be inaccurate, incomplete, out of date or unverifiable. Originating agencies providing terrorism-related data to TFC will be advised in writing if their data is suspected or found to be erroneous, include incorrectly merged information, or lack adequate context such that the rights of the individual may be affected.

7. The TFC will use written or documented electronic notification to inform recipient agencies when information previously provided by the TFC is deleted or changed by the center or the originating agency because it is determined to be inaccurate, includes incorrectly merged information, or lack adequate context such that the rights of an individual may be affected.

H. COLLATION AND ANALYSIS

1. Information acquired by the TFC or accessed from other sources will only be analyzed 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 disseminated by the TFC will be authorized on a "need to know, right to know" basis, and will be provided in accordance with applicable laws, rules, and regulations on the state, local, and federal levels. Furthermore, all TFC personnel who receive, handle, or have access to the TFC data will be trained as to those regulations.

3. All stakeholder agencies and other law enforcement/homeland security personnel having access to the TFC data agree to abide by the following rules:

   A. TFC's data will be used only in support of official law enforcement or public safety activities in a manner authorized by the requestor's employer.

   B. Individual passwords will not be disclosed to any other person, except as authorized by TFC management.

   C. Individual passwords of authorized personnel will be changed if the password is compromised or improperly disclosed.

   D. Background checks will be completed on personnel who will have direct access to TFC at a level determined by the Governance Board.

   E. Use of the TFC's data in an unauthorized or illegal manner could result in the personnel being denied further use of the TFC CRMS system, discipline by the requestor's employing agency, and/or criminal prosecution.

   F. The TFC reserves the right to deny access to any TFC data user who fails to comply with the applicable restrictions and limitations of TFC policy.

   G. The information analyzed is that information as listed in Section E. of this privacy policy.

   H. The purpose of acquiring and accessing sources for analysis is for the development and dissemination of criminal and/or terrorist related information.

I. MERGING RECORDS

Records about an individual or organization from two or more sources will not be merged unless there is sufficient identifying information to reasonably conclude that the information is about the same individual or organization. The set of identifiers sufficient to allow merging will consist of all available attributes that can contribute to higher accuracy of match. If the matching requirements are not fully met but there is an identified partial match, the information may be associated if accompanied by a clear

statement that it has not been adequately established that the information relates to the same individual or organization.

J. SHARING AND DISCLOSURE

1. Credentialed, role-based access criteria will be used to control: what information a class of users can have access to; what information a class of users can add, change, delete or print, and to whom the information can be disclosed and under what circumstances.

2. The TFC 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

3. Access to or disclosure of records retained by the TFC will only be provided to persons within the TFC 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 whom the person is working. An audit record will be kept of access by or dissemination of information to such persons.

4. As long as information constitutes active criminal investigation or active criminal intelligence information, or is otherwise within the scope of an applicable exemption or confidentiality provision of Tennessee law, information gathered and records retained by the TFC, to include ISE-SAR information and those records within the CIMS and the FBI eGuardian system will not be released to the public. ISE-SAR information posted to the FBI eGuardian system by the TFC may be disclosed to a member of the public only if the information is defined by law to be public record or otherwise appropriate for release to further the TFC mission and is not exempt from disclosure by law.

5. Participating agencies may not disseminate the TFC information received from the TFC without approval from the originator of the information.

6. Records retained by the TFC may be accessed or disseminated to those responsible for law enforcement, public protection, public health and safety purposes, prosecutions, or justice purposes derived from criminal investigations or prosecutions, and only in the performance of official duties in accordance with applicable laws and procedures. An audit record will be kept of access by or dissemination of information to such persons.

7. Stakeholder and other law enforcement or government agencies providing data to or through CRMS or CIMS remain the owners of the data contributed. These agencies are responsible for the quality and accuracy of the data accessed by the TFC. TFC personnel will endeavor to identify inconsistencies between information received through database searches and information crosschecked with other data systems and open source information in a manner consistent with the Standard Operating Procedures. User agencies and individual users are responsible for the purging and updating of the data provided to the TFC.

8. Information obtained from or through the TFC can only be used for lawful purposes.

9. A lawful purpose means the request for data can be directly linked to a law enforcement agency's active criminal or terrorism investigation, or is intended to assist in an intervention to prevent a possible criminal/terrorist act or threat to public safety.

10. Unauthorized access or use of the TFC information resources is forbidden.

11. User agencies and individual users are responsible for compliance with respect to use and further dissemination of such information.

12. Information gathered and records retained by TFC may be accessed or disseminated for specific purposes upon request by persons authorized by law to have such access and only for those users or purposes specified in the law. An audit record will be kept of access by or dissemination of information to such persons.

13. Information gathered and records retained by the TFC 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 agency mission and is not exempted from disclosure by law. Such information may only be disclosed in accordance with the law and procedures applicable for this type of information or when there is a legitimate need. An audit record will be kept of all requests and of what information is disclosed to a member of the public.

14. Information obtained from the CRMS or through the TFC will not be used or publicly disclosed for purposes other than those specified in the Memorandum of Understanding (MOU) signed with the participating agency.

15. Regardless of the Memorandum of Understanding, information cannot be:

    A. sold, published, exchanged, or disclosed for commercial purposes;

B. disclosed or published without prior approval of the contributing agency (with the exception of information released through Public Records Act requests and/or other disclosures required by applicable law); or

C. disseminated to unauthorized persons.

D. granted to agencies without a valid Originating Agency Identifier (ORI) issued from the FBI.

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

A. Public records required to be kept confidential by law are exempted from disclosure requirements under Tenn. Code Ann. 10-7-501, et seq;

B. Investigatory records of law enforcement agencies are exempted from disclosure requirements under 28 CFR Part 23. However, certain law enforcement records must be made available for inspection and copying under Tenn. Code Ann.10-7-501, et seq;

C. 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 possibly under Tenn. Code Ann.§ 39-13-807. This includes a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism or an act of agricultural terrorism under Tenn. Code Ann. § 10-7-504, vulnerability assessments, risk planning documents, needs assessments and threat assessments;

D. Protected federal, state, local, or tribal records, which may include records owned or controlled by another agency; and,

E. A violation of the nondisclosure agreement.

17. The TFC shall not confirm the existence or nonexistence of information to persons or agencies ineligible to receive the information to include CIMS records or ISE-SAR information, unless otherwise required by law.

18. Personally identifiable information (such as social security numbers) will be removed from disseminated products as appropriate, for example, when dissemination includes non-law enforcement entities.

K. REDRESS

1. Any non-law enforcement request for information is subject to applicable state, federal and local laws. Tennessee Public Records Act requests, filed pursuant to

Tenn. Code Ann. §10-7-101, et seq., that are received by TFC, shall be forwarded to the Privacy Officer/Custodian of the Records for answer.

2. Upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity and subject to the conditions specified 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 TFC. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information. Responses to requests 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.

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

   A. Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution [Tenn. R. Crim. P. 16];

   B. Disclosure would endanger the health or safety of an individual, organization, or community [Tenn. Code Ann. § 10-7-504];

   C. The information is in a criminal intelligence system subject to 28 CFR Part 23;

   D. The information relates to information protected under Tenn. Code Ann. §10-7-504;

   E. TFC does not have a right to disclose the information pursuant to federal or state law or regulation.

   If information does not originate with the TFC, the TFC will release it pursuant to the Tenn. Code Ann. § 10-7-501, et seq., unless the information is exempt from disclosure under other state or federal law or regulation.

4. The data maintained by the TFC is obtained through participating stakeholder agencies, federal agencies, and open source resources. Individual users of the TFC information are solely responsible for the interpretation of any information developed in the research process. Additionally, it is the responsibility of the user to assess and confirm the accuracy, validity, and completeness of all information and/or intelligence obtained prior to official action being taken in full or in part.

5. If an individual has objections to the accuracy or completeness of the information retained about him or her within a system under the center's control that has been disclosed, the individual will be informed of the procedure for requesting corrections. Requests shall be submitted to TFC Privacy Officer at the following

addresses: TFC Privacy Officer, TBI Professional Standards Unit, 901 R.S. Gass Boulevard, Nashville, TN 37216 and at TFC Privacy Officer, TDOS Legal Division, 1150 Foster Avenue, Nashville, TN 37243. A record will be kept of all requests for corrections.

6. If an individual has an objection to the accuracy or completeness of information about him or her that originates with another agency and has been disclosed, Privacy Officer or designee will notify the originating agency of the correction request and coordinate with them to ensure that the individual is provided with correction request procedures. When the complaint pertains to the correction of a record that has been disclosed to the requester, the originating agency must either consent to the correction, remove the record, or assert a basis for denial in accordance with Tenn. Code Ann. §10-7-501, et seq.. This must be done in sufficient time to permit compliance with deadlines found within Tenn. Code Ann. §10-7-501, et seq. A record will be kept of all correction requests.

7. Where the information originated outside of the TFC, upon a written request by the head of the originating agency or his or her official designee, the TFC will assist in any investigation into an objection regarding the accuracy or completeness of information.

8. The ISE Privacy Guidelines require the TFC to adopt redress procedures when a complaint involves records that have not been disclosed to the complainant under applicable law.

9. If an individual has complaints or objections to the accuracy or completeness of terrorism-related information that has not been disclosed to him or her and which is alleged to have caused the complainant demonstrable harm, the TFC Privacy Officer or designee will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints may be directed to the Privacy Officer (or designee) at the following addresses: TFC Privacy Officer, TBI Professional Standards Unit, 901 R.S. Gass Boulevard, Nashville, TN 37216 and at TFC Privacy Officer, TDOS Legal Division, 1150 Foster Avenue, Nashville, TN 37243. The Privacy Officer or designee will notify the originating agency, if any, of the complaint within 10 days and coordinate with them to resolve the complaint. The originating agency or the Privacy Officer (for Center originated information) must confirm the accuracy of the record, make any needed additions or corrections, or request removal of the record within a reasonable time, not to exceed 30 days, after which the TFC will no longer share the information until such time as the complaint is resolved. A record will be kept of all complaints and the resulting action taken in response to the complaint.

10. Where the ISE information originated from outside the TFC, upon a written request by the head of the originating agency or his or her official designee, the TFC will assist in any investigation into a complaint or objection regarding the accuracy or completeness of information.

11. To delineate ISE information from other data, the TFC maintains records of the ISE originating agencies the center has access to, as well as audit logs, and employs system mechanisms whereby the source is identified within the information record.

12. The individual to whom information has been disclosed will be given reasons if requests for corrections are denied by the center or originating agency. The individual will also be informed of the procedure for the appeal when the center or originating agency has declined to correct challenged information to the satisfaction of the individual about whom the information relates.

L. SECURITY SAFEGUARDS

1. The Assistant Director of Information System at TBI shall be designated and trained to serve as the TFC's Fusion System security officer.

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

3. The TFC 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.

4. The Governance Board or its designee will identify technical resources to establish a secure facility for TFC operations with restricted electronic access, security cameras, and alarm systems to guard against external breach of the facility. In addition, the Governance Board or its designee will identify technological support to develop secure internal and external safeguards against network intrusion of data systems

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

6. Research of data sources is limited to those individuals who have been selected, approved, and trained accordingly. Access to information contained within the TFC will be granted only to fully authorized personnel who have been screened with state and national fingerprint-based background checks, as well as any additional background standards established by the Governance Board.

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

8. The TFC will utilize data logs to maintain audit records of requested and disseminated information.

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

10. TFC personnel or other authorized users shall report violations or suspected violations of center policies relating to protected information to TFC's Privacy Officer for action up to and including revocation of the user's Memorandum of Understanding and reporting to the Governance Board.

11. TFC personnel will follow the data breach notification guidance set forth in Tenn. Code Ann. § 47-18-2107.

12. Queries made to data applications will be documented by identifying the user initiating the query. When such information is disseminated outside of the requesting agency by the Privacy Officer, documentation of such dissemination will occur, capturing updated information and providing an appropriate audit record as required by applicable law which shall be maintained by the Privacy Officer. Secondary dissemination of information can be sent 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:

    A. Date of release.

    B. The subject of the information.

    C. To whom the information was released (including address and telephone number).

    D. An identification number or other indicator that clearly identifies the data released.

    E. The purpose for which the information was requested.

13. The Governance Board will be responsible for facilitating any internal or special audits, and for investigating misuse of information systems. All confirmed or suspected violations of policies will be reported through the Privacy Officer to the Governance Board. Individual users of TFC information remain responsible for the appropriate use of TFC information. Each user and each participating agency within the TFC is required to abide by this Privacy Policy in the use of information disseminated. Failure to abide by the restrictions for the use of the

TFC data may result in the suspension or termination of user privileges and discipline imposed by the user's employing agency, and/or criminal prosecution.

M. INFORMATION RETENTION AND DESTRUCTION FOR CRIMINAL INTELLIGENCE INFORMATION

1. Criminal Intelligence Information

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

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

   C. The TFC will delete information or return it to its source, unless it is validated to demonstrate continued criminal predicate, every five (5) years.

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

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

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

   G. Information not validated to demonstrate continued criminal predicate within the review period will be purged.

2. Consolidated Records Management System

   A. The Consolidated Records Management System (CRMS) is a database repository containing activity records submitted by law enforcement agencies and criminal justice organizations, interactively updated into the CRMS, to include additions, updates, or deletions of records as submitted by the originating agency. The CRMS is not subject to 28 C.F.R. Part 23.

B. Agencies contributing data to the CRMS are solely responsible for determination of retention and destruction according to applicable state, local, and federal laws and agency policies.

C. The TFC will not add, change, or delete data contained in the CRMS.

3. Tips and leads, SAR, and FBI eGuardian system information

A. Tip and Leads received within the CRMS will be retained as uploaded by the originating agency for an indefinite period of time.

B. Tips and leads or SARs that are moved into the CIMS will be retained for a period of five (5) years in order to work an unvalidated tip, lead, or SAR information to determine its credibility 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.

C. FBI eGuardian system information will be retained for a period of five (5) years in order to work an unvalidated tip, lead, or SAR information to determine its credibility 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.

N. ACCOUNTABILITY AND ENFORCEMENT

1. It is the intent of the TFC and participating agencies to be open with the public concerning data collection practices when such openness will not jeopardize ongoing criminal/terrorist investigative activities. TFC shall refer appropriate queries to the originating agency of information as the entity to address any concern about data accuracy and quality, when this can be done without compromising an active inquiry or investigation. All other inquiries shall be referred to the Privacy Officer/Custodian of the Records.

2. All agencies participating in the TFC will make this Privacy Policy available for public review. The TFC will post this Privacy Policy on the public web site of the Tennessee Bureau of Investigation and the Tennessee Department of Safety and Homeland Security and make it available to any interested party.

3. Queries made to data applications will be logged into the data system identifying the user initiating the query, dissemination and reason for the request.

4. The TFC data logs will be utilized to maintain an audit record of requested or disseminated information.

5. The TFC will provide a copy of this policy to all agency and non-agency personnel who provide services and will require written acknowledgement of receipt of this policy and agreement of compliance to this policy and the provisions it contains.

6. The TFC will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with their systems, in provisions of this policy and applicable law. This will include logging access of these systems and periodic auditing of these systems, as to not establish a pattern of the audits. These audits will be mandated at least quarterly and conducted by the TBI Information Systems Division and a record of the audit will be maintained by TFC Directors or designee.

7. TFC personnel or other authorized users shall report violations or suspected violations of center policies relating to protected information to the center's Security Officer.

8. The TFC will annually conduct an audit and inspection of the information contained in its criminal intelligence system, including the CIMS, Tips and Leads, SARs, and FBI eGuardian SARs. The audit will be conducted by an independent panel comprised of 3 or more individuals selected by the Governance Board. This independent panel has the option of conducting a random audit without announcement, at any time and without prior notice to TFC. All audits will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the center's criminal intelligence system. The panel will immediately report audit findings to the Governance Board. Audits of data uploaded to the CRMS are the responsibility of the originating agency. TFC will provide assistance in such originating agency audit if requested.

9. The TFC's Legal Working Group will annually review and update the provisions protecting privacy, civil rights, and civil liberties contained within this policy and make appropriate changes in response to changes in applicable law, changes in technology, changes in the purpose and use of the information systems and changes in public expectations.

10. The TFC will follow the data breach notification guidance set forth in Tenn. Code Ann. § 47-18-2107.

11. The TFC reserves the right to restrict the qualification and number of personnel having access to center information and to suspend or withhold service to any personnel violating the privacy policy. The center reserves the right to deny access to any participating agency user who fails to comply with the applicable restriction and limitation of the TFC privacy policy.

12. Upon receiving a report that TFC personnel, a participating agency, or an authorized user is in noncompliance with the provisions of this policy regarding the gathering, collection, use, retention, destruction, sharing, classification, or disclosure of information, the TFC will initiate an investigation into the report to determine if TFC personnel, a participating agency, or an authorized user was in noncompliance.

    A. If TFC personnel are found to be in noncompliance, the following actions will occur:

        (1) Forward the investigation results to personnel's appointing authority for appropriate action or discipline as may be required and conducted under the employing agency's applicable laws and regulations;

        (2) Suspend or discontinue access to information to the personnel, if necessary, until a determination regarding appropriate disciplinary measures, if any, is made;

        (3) Assist the appropriate agency with any disciplinary actions and/or hearings as may be necessary; and,

        (4) Refer the matter to appropriate authorities for criminal prosecution, as necessary.

    B. If a participating agency is found to be in noncompliance, the following actions will occur:

        (1) Forward the investigation results to the TFC Governance Board and the head of the participating agency;

        (2) Suspend participating agency access or terminate the MOU, if necessary based on the severity of the noncompliance; and,

        (3) Refer the matter to appropriate authorities for criminal prosecution, as necessary.

    C. If an authorized user is found to be in noncompliance, the following actions will occur:

        (1) Forward the investigation results to the head of the authorized user's employing agency;

        (2) Suspend or discontinue access to information by the authorized user, if necessary, until a determination regarding appropriate

disciplinary measures, if any, is made by the employing agency under any applicable civil service rules or other state or federal laws or regulations regarding the authorized user's employment;

(3) Assist the appropriate agency with any disciplinary actions ad/or hearings as may be necessary; and,

(4) Refer the matter to appropriate authorities for criminal prosecution, as necessary.

O. TRAINING

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

   A. All TBI and TDOSHS personnel assigned to the TFC.

   B. All users who are assigned to the TFC but not employed by either TBI or TDOSHS or contractor.

   C. Personnel providing information technology service to the TFC.

   D. Staff in other public agencies or private contractors providing service to TFC.

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

3. TFC's privacy policy training program will cover:

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

   B. Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the TFC;

   C. How to implement the policy in the day-to-day work of the user, whether a paper or systems user;

   D. The impact of improper activities associated with an infraction accessible within or throughout the agency;

E. Mechanisms for reporting violations or center privacy-protection policies; and,

F. The nature and possible penalties for policy violations, including possible transfer, dismissal, criminal liability and immunity, if any; and,

G. Originating and participating agency responsibilities and obligations under applicable law and policy.