U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

October 13, 2011

Commander Marco Spalloni
MATRIX – El Paso Fusion Center
El Paso Police Department
911 N. Raynor St.
El Paso, Texas 79903

Dear Commander Spalloni:

The Intelligence Reform and Terrorism Prevention Act of 2004, as amended by the Implementing Recommendations of the 9/11 Commission Act of 2007, established an information sharing environment for the sharing of terrorism-related information while protecting the privacy, civil rights, and civil liberties of individuals. The *Guidelines to Ensure that Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment* ("ISE Privacy Guidelines") require relevant entities to have a written privacy protection policy in place that is "at least as comprehensive" as the ISE Privacy Guidelines.

In my capacity as a co-chair of the Privacy and Civil Liberties Subcommittee of the Information Sharing and Access Interagency Policy Committee, I have reviewed the MATRIX – El Paso Fusion Center node privacy policy and recognize it to be "at least as comprehensive" as the ISE Privacy Guidelines. Your privacy policies should be renewed and updated as necessary based on any future changes to the ISE Privacy Guidelines.

Completion of this written privacy policy is an important first step in the implementation of a strong privacy protection framework, to include training of personnel in privacy and civil liberties protections. In fostering trust among the public and your partners, I urge you to make this policy available to the public through a variety of different channels, to include electronic means. Agencies must supply a copy of this privacy policy upon request, but I also recommend you post it on any public facing website your center maintains and be prepared to discuss it as you liaise with your local communities.

Finally, I strongly recommend that you begin preparing a Privacy Impact Assessment (PIA) or updating an existing PIA, if applicable. A PIA is a vital tool used to evaluate possible privacy risks and to mitigate identified risks to the privacy, civil rights, and civil liberties of individuals. The Global Justice Information Sharing Initiative's *Guide to Conducting Privacy Impact Assessments for State, Local, and Tribal Information Sharing Initiatives* can be found at http://www.it.ojp.gov/default.aspx?area=privacy&page=1295 and is a useful resource in PIA development.

Should you have any questions with regard to privacy issues, please feel free to contact the DHS Privacy Office on behalf of the Privacy and Civil Liberties Subcommittee at 703-235-0780.

Sincerely,

John W. Kropf
Deputy Chief Privacy Officer
Department of Homeland Security

cc: Alexander W. Joel, ODNI CLPO
Nancy C. Libin, DOJ CP&CLO
Margo Schlanger, DHS Officer for Civil Rights and Civil Liberties

EL PASO POLICE DEPARTMENT

"MATRIX"

FUSION CENTER

PRIVACY POLICY

A. PURPOSE

A.1 PURPOSE STATEMENT

The purpose of this policy is to provide relevant state, local and private sector partners with guidelines, standards, policies and procedures for the operation of the El Paso Police Department MATRIX Fusion Center. This policy is designed to bring about an equitable balance between the privacy, civil rights, and civil liberties of individuals and organizations and the needs of law enforcement to collect and disseminate criminal justice information and intelligence on persons or organizations involved in criminal activity. This Privacy Policy embraces the eight privacy design principles or "Fair Information Principles" (see definition in Appendix A) developed by the Organization for Economic Co-operation and Development (OECD) and contained within its "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," and shall be used to guide the policy wherever applicable.

A.2 MISSION STATEMENT

The Mission of the El Paso Police Department FUSION CENTER (MATRIX – Multi Agency Tactical Response Information eXchange) is to serve as an all-crimes/all-hazards tactical information and intelligence hub for the El Paso Police Department and *Participating Agencies*. This integrated, multi-disciplinary information sharing network will seek, collect, analyze and disseminate information and intelligence to stakeholders in a timely manner in order to protect the citizens and critical infrastructure of El Paso while preserving the privacy and U.S. and Texas Constitutional rights of individuals.

B. POLICY APPLICABILITY AND LEGAL COMPLIANCE

B.1 COMPLIANCE AND GOVERNANCE

B.1.1. The El Paso Police Department implements these operating policies and procedures to govern the FUSION CENTER and *Participating Agencies* in the collection, submission, analysis, query, dissemination, retention, and security of *Records* in the various electronic intelligence information systems maintained by the FUSION CENTER. The purpose of this activity is to support the goals of the FUSION CENTER, which are:

a) strengthen Information and Intelligence Sharing and Support to El Paso Police Department Patrol Officers;

b) disrupt Significant Criminal Organizations;

c) provide increased investigative support to the El Paso Police Department; and,

d) support area law enforcement, public and private sector stakeholders to better forecast and identify emerging crimes, public health and quality of life trends.

B.1.2. All FUSION CENTER personnel, *Participating Agency* personnel, personnel providing information technology services to the agency, private contractors, and other authorized users must be in compliance with applicable constitutional and statutory laws (including but not limited to those outlined in Appendix B), and this privacy policy, concerning the laws protecting privacy, civil rights, and civil liberties in the seeking, gathering, use, analysis, retention, destruction, sharing, securing and disclosure of information and intelligence to FUSION CENTER personnel, governmental agencies and participating justice and public safety agencies, as well as to private contractors and the general public.

B.1.3. The gathering of information in support of these goals is vital to achieving success but must be balanced and guided by the need and responsibility to preserve the privacy rights of individuals, civil rights and civil liberties.

B.1.4. The FUSION CENTER will provide a printed or electronic copy of this policy to all FUSION CENTER and non-agency personnel who provide services

and will require both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and the provisions it contains.

B.1.5. The FUSION CENTER has adopted internal operating procedures and policies that are in compliance with applicable U.S. and Texas Constitutional and statutory laws (see Appendix B for a list of State and Federal laws) protecting privacy, civil rights, and civil liberties in the gathering, use, analysis, retention, destruction, sharing, securing and disclosure of information.

B.1.6. The FUSION CENTER will provide a printed or electronic copy of this policy upon request by any person, corporation, or organization.

B.2 PROTECTIONS DEFINED

B.2.1. The United States was created with the principles of protecting certain privileges from government intrusion as guaranteed rights, which has led to the further refining of concepts such as right to privacy that developed from case law and statutory protections from government and others overreach into a person's life. FUSION CENTER articulates and defines the intention and commitment to protect:

a) individual "privacy" which refers to individuals' interest in preventing the inappropriate collection, use and release of personally identifiable information;

b) against the use of inappropriate or illegal means used to gather personal data and personal conduct and the inappropriate release of information that causes embarrassment, shame or loss;

c) personally identifiable information which is one or more pieces of information, such as personal characteristics and unique identifiers, that when considered together or when considered in the context of how it is present or how it is gathered is sufficient to specify a unique individual;

d) civil rights, which are those fundamental freedoms and privileges guaranteed by the 13th and 14th Amendments to the U.S. Constitution and by subsequent acts of Congress, including civil liberties, due process, equal protection of the laws, and freedom from discrimination; and,

e) civil liberties as those fundamental individual rights, such as freedom of speech and religion, protected by law against unwarranted governmental interference.

B.2.2. The FUSION CENTER intends to establish a foundation for protection by acknowledging these protections, by providing transparency in establishing processes and procedures for operation, by ensuring adequate training and understanding for users and by having sufficient audit and oversight to ensure compliance.

C. GOVERNANCE AND OVERSIGHT

C.1 Primary responsibility for the operation of the FUSION CENTER, its justice systems, operations, and oversight of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing, securing or disclosure of information; and the enforcement of this policy is assigned to the Fusion Center Commander of the El Paso Police Department.

C.2 This policy was developed and reviewed by the El Paso Police Department, the FUSION CENTER STEERING COMMITTEE, the City of El Paso Legal department, and the United States Department of Justice; furthermore, a review of this policy will be conducted annually by the Privacy Officer, as described and defined in Section N.2.10. The FUSION CENTER STEERING COMMITTEE and the City of El Paso Legal department will review, counsel, and consent to the changes prior to the revised policy's implementation.

C.3 The FUSION CENTER STEERING COMMITTEE will provide a printed or electronic copy of this policy upon request to any person, corporation, or organization making such a request.

C.4 The FUSION CENTER's Administrator is designated and trained to serve as the center's Privacy Officer. The Privacy Officer serves as staff to the FUSION CENTER STEERING COMMITTEE, receives reports regarding alleged errors and violations of the provisions of this policy, receives and coordinates complaint resolution under the center's redress policy to ensure that privacy protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy-enhancing technologies. The Privacy Officer can be contacted using the following methods:

C.4.1. Email – privacy_fusion@elpasotexas.gov

C.4.2. U.S. Mail – Privacy Officer, El Paso Fusion Center, 911 N. Raynor St., El Paso, Texas 79903

C.4.3. Telephone – (915) 564-7100

C.5 The FUSION CENTER'S Privacy Officer ensures that the enforcement procedures and sanctions described and defined in Section N.3 are adequate and enforced.

D. DEFINITIONS

The primary terms and definitions used in this policy are set forth in Appendix A.

E. INFORMATION

E.1 GUIDING STATUTES AND POLICY APPLICABILITY

The FUSION CENTER acknowledges the application of certain law, statutes and policies which may affect the Mission and Goals of the FUSION CENTER and its operation, including United States Constitution, United States Federal Code of Regulations - 28 CFR Part 23, regarding intelligence information systems; the Texas Constitution, Texas Code of Criminal Procedure Chapter 61, and amendments contained in Senate Bill 418 81st Legislature, regarding Gang Intelligence and 28 CFR standards; Chapter 421 of the Texas Government Code, regarding the Department of Public Safety and the collection of terrorist and Homeland Security information; Chapter 552 of the Texas Government Code, regarding open government; and the Department of Homeland Security published Baseline Capabilities Guidelines for Fusion Centers. (See also Appendix B – State and Federal Law).

The development of Fusion Center processes and operating procedures will be guided by privacy design principles from *Fair Information Principles;* which shall also serve to guide personnel in the application of guiding statutory authority. These principles are:

E.1.1. *Purpose Specification* – Define agency purposes for information to help ensure agency uses of information are appropriate.

E.1.2. *Collection Limitation* – Limit the collection of personal information to that required for the purposes intended.

E.1.3. *Data Quality* – ensure data accuracy.

E.1.4. *Use Limitation* – Ensure appropriate limits on law enforcement use of personal information.

E.1.5. *Security Safeguards* – Maintain effective security over personal information.

E.1.6. *Openness* – Promote a general standard of openness and transparency regarding practices, process and policy regarding collecting, disseminating and archiving personal information.

E.1.7. *Individual Participation* – Allow individuals reasonable access and opportunity to correct errors in their personal information held by the agency.

E.1.8. *Accountability* – Identify, train and hold participating personnel accountable for adhering to Fusion Center information quality and privacy policy standards.

E.2 LIMITATIONS & STATEMENT OF INTENT

E.2.1. The FUSION CENTER is operated and managed by the El Paso Police Department as an information and intelligence center. The FUSION CENTER has the potential to come into contact with a broad scope of both public and private information and data. The FUSION CENTER will not seek, collect, analyze, or disseminate information or data that does not support the identified goals of law enforcement, disrupt or prevent crime, terrorism or violent acts.

E.2.2 The FUSION CENTER will prohibit its employees and will not seek or retain, and information-originating agencies hereby agree not to submit, information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, or sexual orientations.

E.2.3 The FUSION CENTER will only seek, retain, analyze or disseminate information that:

a) is based on a criminal predicate or possible threat to public safety; 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 conduct or activity; or

c) is relevant to the investigation and prosecution of suspected criminal incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime; or

d) is useful in a crime analysis or in the administration of criminal justice and public safety; and

e) is obtained from a reliable source and is verifiable or limitations on the quality of the information are identified; and

f) was collected in a fair and lawful manner.

E.3 INFORMATION IN GENERAL

E.3.1 The FUSION 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*s (SAR).

E.3.2 This policy applies to protected information about all individuals and organizations (as expressly included by law or policy) obtained by the FUSION CENTER in furtherance of its analytical and information sharing missions. Information that furthers an administrative or other non-analytical purpose (such as personnel files, or information regarding fiscal, regulatory or other matters associated with the operation of the FUSION CENTER) will not be subject to the provisions of this policy.

E.4 INFORMATION SYSTEMS

E.4.1. The FUSION CENTER, thru the El Paso Police Department, will have access to and utilize:

a) a Records Management System (RMS) for the collection and reporting of certain crimes and incidents.

b) a criminal investigative reporting system for the case management of criminal investigations.

c) an intelligence database to document, categorize, label, and store intelligence information that is compliant with 28 CFR Part 23.

d) various government, public, institutional, private and commercial databases providing information to augment existing Records and information.

E.4.2. The FUSION CENTER will collect, manage and analyze information related to the collection of *Suspicious Activity Report*s (SAR).

E.4.3. The FUSION CENTER will also have access to certain surveillance systems that allow the visual electronic surveillance of public areas that are protected in the region.

E.4.4. The FUSION CENTER 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, to include personal data on any individual entitled to protection under federal, state, local, and tribal law, and to the extent expressly provided in this policy, includes organizational entities.

b) The information is subject to applicable laws restricting access, use, or disclosure based on information sensitivity or classification, including but not limited to the U.S. and Texas Constitutions, applicable federal law, and state law, including Texas Government Code Chapter 552 Public Information Act.

E.4.5. The FUSION CENTER will keep a record of the source of all information sought and collected by the center and will apply additional labels to each *Record* with the appropriate metadata: date and time the information was originally received; the nature of the information, i.e., *suspicious activity report*, *tips and leads,* criminal history, intelligence information, criminal case report, conditions of supervision, case management, external database source, et cetera; the categories of the appropriate *Intelligence Source Reliability* and *Intelligence Information Validity* consistent with 28 CFR Part 23 guidelines; and, the information classification, i.e., Sensitive, Confidential, Unclassified.

E.4.6. At the time a decision is made by the FUSION CENTER 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:

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 or his or her civil rights and civil liberties.

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

E.4.7. The labels assigned to existing information under Section E.4.4 will be reevaluated whenever:

a) New information is added that has an impact on access limitations or the sensitivity of disclosure of the information.

b) There is a change in the use of the information affecting access or disclosure limitations; for example, the information becomes part of court proceedings for which there are different public access laws.

E.4.8. The FUSION CENTER will only utilize databases and contract with commercial database entities that provide an assurance that their methods for gathering personally identifiable information comply with applicable local, state, tribal, territorial, and federal laws, statutes, and regulations and that these methods are not based on misleading information-gathering practices.

E.5 PUBLIC SURVEILLANCE SYSTEMS

E.5.1. The FUSION CENTER may access data from certain electronic camera or surveillance systems for the enhancement of overall protection of the public, critical infrastructure, key resources or public areas easily accessed by the general public. Unless installed pursuant to an ongoing criminal investigation and appropriate court order, no such systems will be placed or installed to view an area where there is a reasonable expectation of privacy by any member of the general public. No data or images from these systems may be accessed or used by any person except for the legitimate protection of the public or the furtherance of an approved criminal investigation.

E.5.2. Any data or images stored or retained by the FUSION CENTER thru recording of or from the use of any of these systems may only be retained for a period of 24 months unless specifically identified by *Reasonable Suspicion* standards as related to criminal activity. Without such correlation or analysis, all data or images must be purged and a permanent log or record kept identifying the person and method used for purging. Any query or request for dissemination of stored data from these systems by any person except for furthering an authorized criminal investigation will be refused. Permanent logs regarding any request for dissemination and any such dissemination or refusal; along with the method and identification of the person making routine destruction will be available upon request at the FUSION CENTER offices.

E.6 TIPS, LEADS AND SUSPICIOUS ACTIVITY REPORTING

E.6.1. The FUSION CENTER may access unsubstantiated or uncorroborated information or data from inside or outside the agency that alleges or indicates some form of possible criminal activity. This type of information or data is generally referred to as *tips and leads* and is sometimes referred to as *suspicious activity report* (SAR). However, SAR information should be viewed, at most, as a subcategory of *tips and leads* data.

E.6.2. The FUSION CENTER will receive, collect, analyze, evaluate, retain and secure *tips and leads* and *suspicious activity report* (SAR) information. Moreover, the FUSION CENTER will:

a) identify trends and patterns of potential events which are threats to our nation, state or jurisdiction and its citizens to improve the effectiveness of the criminal justice community response to such events and bring closure to events and information which do not pose such threats;

b) in accordance with the understanding that information may not immediately meet a *Reasonable Suspicion* standard and thus not be compliant with 28 CFR, limit the dissemination of such raw information that has not been analyzed or is not able to be labeled or elevated to finished criminal intelligence, using the same (or a more restrictive) access or dissemination standard that is used for data the rises to the level of *Reasonable Suspicion* (For example, "need-to-know" and "right-to-know" access or dissemination for personally identifiable information);

c) professionally analyze and evaluate to determine if the record can be elevated to meet 28 CFR guidelines as finished intelligence by "reasonable suspicion" standards and that the analysis conclusion is supported by relevant documentation before it can be considered for submission to an intelligence file or Records system;

d) retain and secure in an intelligence file, information elevated to meet 28 CFR guidelines as finished intelligence, using the same storage method used for data that rises to the level of reasonable suspicion and includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information;

e) delete if the basis for submission includes only political, religious, or other First Amendment activities or the expression of personal opinions;

f) delete regardless of the criminal activity involved, if the Authorized User making an assessment has good reason to believe that the supporting information was illegally obtained;

g) delete unless it:

(1) serves to identify an individual or organization that is involved in terrorism; or

(2) shows a nexus to violating a criminal law of the State, the United States, or any jurisdiction in the United States that would be a violation of a criminal law of Texas; or

(3) meets the legal definition of gang activity under State or federal law; or,

(4) poses a clear and present threat to public order and safety.

E.6.3. The FUSION CENTER will enforce internal policies that will automatically purge tips, leads, or SAR *Record*s which are not acted upon or evaluated within 5 years.

E.6.4. The FUSION CENTER will enforce policies regarding the purging of personal identifying information which has expired according to 28 CFR standards (5 year retention or purge unless validated for an additional retention period) or deemed as not meeting minimum standards for accuracy or submission.

E.6.5. The report validation processes may include research of suspect information and personal identifying information to support or refute criminal activity. These validation processes will necessarily involve contrast and comparison from other private and public data sources that attempt to identify, establish or validate reports of suspected persons or events. There should be no merging of personally identifying data from other data sources that establish identity or criminal behavior unless multiple criteria are validated as matching.

E.6.6. While the FUSION CENTER may store *Record*s supported by documented information, it also may contain anonymous reports and potential erroneous reports. Therefore, it is not designed to provide a *Record* upon which to base an official action. The FUSION CENTER merely identifies that information was received which must be validated to assess the information supporting the *SAR* record. While this supporting information may be used to justify official action, the tip, lead or *SAR* record itself may not be used to provide:

a) probable cause for a warrantless arrest;

b) probable cause in an affidavit for an arrest or search warrant;

c) proof in a court procedure for enhancing the penalty for a crime; or,

d) used for background or employment application purposes.

E.6.7. The FUSION CENTER will apply the same labeling standards as defined and described in Section E.4.4 and E.4.5 to tips, leads, and SAR information.

E.6.8. The Fusion Center will apply the same source of information standards as defined and described in Section E.12.

E.6.9. The FUSION CENTER will, for a tip, lead or SAR that rises to the level of reasonable suspicion, enter the record into a criminal intelligence information system.

E.6.10. For all tip, lead, and SAR information, the FUSION CENTER will:

a) Allow access to or disseminate the information using the same access or dissemination standard that is used for criminal intelligence information.

b) 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.

c) Immediately refer a SAR to the FBI's Joint Terrorism Task Force Liaison when a SAR has been determined, pursuant to a two-step process established in the *Information Sharing Environment* Functional Standard (ISE-FS), to have a potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism).

E.6.11. The FUSION CENTER will ensure that only an *Authorized User,* trained in the ISE-FS (ISE-FS-200) – including ISE-SAR Criteria Guidance Matrix – will conduct the validation process for a SAR. The FUSION CENTER Commander or designee will be responsible for making the final determination for ISE-SAR submission.

E.6.12. The FUSION CENTER adheres to the current version of the ISE-SAR Functional Standard for its suspicious activity reporting (SAR) process, including the use of a standard reporting format and commonly accepted data collection codes and a sharing process that complies with the ISE-SAR Functional Standard for suspicious activity potentially related to terrorism.

E.6.13. The FUSION CENTER will 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 constitutional rights, including personal privacy and other civil liberties, and civil rights.

E.6.14. The FUSION CENTER will identify and review protected information that may be accessed from or disseminated by the center prior to sharing the information through the Information Sharing Environment. Further, the center will provide notice

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

E.7 CRIMINAL INTELLIGENCE SYSTEMS

E.7.1 A criminal intelligence file consists of stored information on the activities and associations of:

a) Individuals who:

(1) based upon reasonable suspicion are suspected of being or having been involved;

(2) are in the actual or attempted planning, organizing, threatening, financing, or commission of criminal acts;

(3) based upon reasonable suspicion are suspected of being or having been involved in criminal activities with known or suspected crime figures.

b) Organizations, business and/or groups which:

(1) based upon reasonable suspicion, are suspected of being or having been involved in the actual or attempted planning, organizing, threatening, financing, or commission of criminal acts; or

(2) that based upon reasonable suspicion are suspected of being or having been illegally operated, controlled, financed or infiltrated by known or suspected crime figures.

E.7.2. Information gathering for intelligence purposes shall be premised on circumstances that provide a reasonable suspicion as defined in 28 CFR, Part 23 entitled "Criminal Intelligence Operating Systems, and in accordance with United States Constitution, the Texas Constitution, Texas Code of Criminal Procedure Chapter 61, and amendments contained in Senate Bill 418 81st Legislature, regarding Gang Intelligence and 28 CFR standards; Chapter 421 of the Texas Government Code, regarding the Department of Public Safety and the collection of terrorist and Homeland Security information; Chapter 552 of the Texas Government Code, regarding open government. (See also Appendix B – State

and Federal Law).

E.7.3 The primary purposes of these criminal intelligence systems are receipt, storage, and sharing of criminal intelligence information. As such the FUSION CENTER will be the repository for all criminal intelligence information maintained by the El Paso Police Department. The FUSION CENTER Commander will be responsible for the management of all criminal intelligence systems and will be the Department designee for managing such systems.

E.7.4 The goal of these criminal intelligence systems is to improve the effectiveness of the criminal justice community by providing for the timely exchange of documented and reliable information.

E.7.5 The El Paso Police Department operates these intelligence systems and supports dissemination to TXGang which are in compliance with 28 CFR Part 23, and Texas CCP Chapter 61, as amended by Texas Senate Bill 418. The FUSION CENTER will not accept non-criminal identifying information for inclusion in an *El Paso Police Department Gang Database* record. In other supported intelligence systems, the FUSION CENTER may choose to include non-criminal persons, who are appropriately labeled as a non-criminal in the report, only where there is a clear and definable relationship that serves to further identify the criminal activities and behavior of the criminal suspect. No *Record* will be created that stands alone with only a non-criminal person.

E.7.6 Any person involved in the submission, query, dissemination, or review of any supported or maintained intelligence systems must be an *Authorized User* with access approved by their respective agency head or designee and the FUSION CENTER'S Administrator.

E.7.7 The submission or retention of information supporting any *Record* must comply with the intelligence guidelines set forth in 28 CFR, including each of the following:

a) An intelligence record must be supported by documentation that contains information relevant to an individual criminal member (based on proper identification criteria) and/or a criminal street gang or organization (based on proper criminal predicate).

b) No political, religious, or other First Amendment activities or the expression of personal opinions may be used as a valid basis for

inclusion in any supported intelligence system, unless the activity satisfies criminal predicate by:

(1) clearly violating a criminal law of the State, the United States, or any jurisdiction in the United States that would be a violation of a criminal law of Texas;

(2) meeting the legal definition of gang activity under State law; or

(3) posing a clear and present threat to public order and safety.

c) Regardless of the criminal activity involved, no *Record* may be retained or submitted if the submitting agency or authorized user has good reason to believe that the supporting information was illegally obtained.

d) Any submitted information identifying an individual or a criminal organization must meet the criminal predicate requirements of reasonable suspicion identified in 28 CFR Part 23 and the criminal activity must represent a significant and recognized threat to the public and:

(1) Are either undertaken for the purpose of seeking illegal power or profits or pose a threat to the life and property of citizens; and

(2) Involve a significant degree of permanent criminal organization; or

(3) Are not limited to one jurisdiction.

E.7.8 The FUSION CENTER and any Participating Agency may not use data obtained from the Fusion Center to populate another intelligence system or other searchable database or to populate *another agency's* databases.

E.7.9 All intelligence systems will code the identifying information of an individual in the index to differentiate a child (under 17 years of age, as defined in Texas Family Code § 51.02. Definitions (2)(A) "Child") from an adult to prevent an infringement of a juvenile's protections under the Texas Family Code § 58.007

Physical Records or Files and Code of Criminal Procedures Article 61 Compilation of Information Pertaining to Criminal Combinations and Criminal Street Gangs.

E.7.10 All other criminal intelligence systems or future intelligence systems will comply with similar FUSION CENTER criminal intelligence policies.

E.8 NATURE OF INFORMATION

In order to accurately classify and categorize information and intelligence, the FUSION CENTER will delineate each *Record* with the nature of information, i.e., *suspicious activity report, tip and lead*, criminal history, intelligence information, criminal case report, conditions of supervision, case management, et cetera.

E.9 INFORMATION CLASSIFICATION

E.9.1 The FUSION CENTER will classify each *Record* in order to protect sources, investigations, and individual's rights to privacy, as well as to provide a structure that will enable the FUSION CENTER to control access to intelligence.

E.9.2 Information received by *Participating Agencies* or other agencies with information classifications attached to them will be reviewed by Fusion Center Commander or designee, who will assign the appropriate classification; however, the FUSION CENTER classification will never be lower than the classification given by *Participating Agencies* or other agencies. All classifications or re-classifications must be approved by the Fusion Center Commander or designee.

E.9.3 Criminal intelligence information is classified according to the following system:

a) Sensitive - intelligence files include those that contain information that could adversely affect an on-going investigation, create safety hazards for officers, informants, or others and/or compromise their identities. Restricted intelligence may only be released by approval of the Fusion Center Commander or the El Paso Police Department Chief of Police to authorized law enforcement agencies with a need and a right to know.

b) Confidential - intelligence that is less than sensitive intelligence. It may be released to El Paso Police Department personnel when a need and a right to know have been established by the Fusion Center

Commander or designee.

c) Unclassified - intelligence contains information from the news media, public records, and other sources of a topical nature. Access is limited to individuals conducting authorized investigations that necessitate this information.

E.10 INFORMATION CATEGORIZATION

The FUSION CENTER will categorize each *Record* with the appropriate *Intelligence Source Reliability* and *Intelligence Information Validity* consistent with 28 CFR Part 23 guidelines, as follows:

E.10.1 Intelligence Source Reliability

	Class Level	Description
a)	A-Reliable	Source's reliability is unquestioned, has been well tested in the past.
b)	B-Usually Reliable	Source's reliability can usually be relied upon as factual. The majority of past information provided has proven to be reliable.
c)	C-Unreliable	Source's reliability cannot be relied upon as factual or is sporadic at best.
d)	D-Unknown	Source's reliability cannot be judged. Source's Authenticity of trustworthiness has not been determined by either experience or investigation.

E.10.2 Intelligence Information Validity

	Class Level	Description
a)	1- Confirmed	The information has been corroborated
b)	2- Probable	The information is consistent with past accounts.
c)	3- Doubtful	The information is inconsistent with past

accounts.

d) 4- Can't be Judged The information cannot be evaluated.

E.11 DISSEMINATION OF INFORMATION

E.11.1 The FUSION CENTER will ensure that an intelligence record is directly disseminated only to an authorized user by: employing safeguards, including a special role-based user ID and initial password; and will only disseminate a *Record* to a *Participating Agency* through a proper query by an *Authorized User* from an authorized computer terminal. Verbal disseminations to any person will require that the FUSION CENTER *Authorized User* reasonably identify the requestor and the *Need to Know* and *Right to Know*.

E.11.2 The FUSION CENTER will label a dissemination of any *Record* or information with the following metadata:

a) date and time the information was originally received and, where feasible, the date its accuracy was last verified;

b) the nature of the information, i.e., *suspicious activity report*, *tip and lead,* criminal history, intelligence information, criminal case report, conditions of supervision, case management, external database source, et cetera;

c) the categories of the appropriate *Intelligence Source Reliability* and *Intelligence Information Validity* consistent with 28 CFR Part 23 guidelines;

d) the *Information Classification*, i.e., Sensitive, Confidential, Unclassified; and,

e) the title and contact information for the person to whom questions regarding the information should be directed.

E.11.3 All information maintained in the *Record* will be released to an authorized user who makes a proper query, without any special restriction on its dissemination beyond the general requirements of 28 CFR, unless the author or entity has specified restrictions.

E.12 INFORMATION CONTRIBUTORS

To the extent possible, all criminal intelligence maintained by the FUSION CENTER must display the names and phone numbers of person and agencies providing the information. A contributor code number may be used if the agency requests anonymity. All contributor code numbers will be maintained by the *Fusion Center Supervisor*. All information obtained from the public domain will be identified by the source of the information, document name, date obtained and page number.

F. ACQUIRING AND RECEIVING INFORMATION

F.1 The FUSION CENTER will ensure that information-gathering (acquisition) and access and investigative techniques used by the FUSION CENTER, participating agencies, and information-originating agencies will remain in compliance with and will adhere to applicable laws and guidance, including, but not limited to:

F.1.1. 28 CFR Part 23, regarding criminal intelligence information.

F.1.2. The OECD Fair Information Principles (under certain circumstances, there may be exceptions to the Fair Information Principles, based, for example, on authorities paralleling those provided in the federal Privacy Act; state, local, and tribal law; or center policy).

F.1.3. Criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) *National Criminal Intelligence Sharing Plan* (NCISP).

F.1.4. Constitutional provisions and administrative rules, as well as regulations and policies that apply to multijurisdictional intelligence and information databases.

F.2 The FUSION 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 potential 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.

F.3 The FUSION CENTER'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, et cetera) and civil liberties (speech, assembly, religious exercise, et cetera) will not be intentionally or inadvertently gathered, documented, processed, and shared.

F.4 *Participating Agencies* that access the FUSION CENTER's information or share information with the center are governed by the laws and rules governing those individual agencies, including applicable federal and state laws.

F.5 The FUSION CENTER will contract only with commercial database entities that provide an assurance that their methods for gathering personally identifiable information comply with applicable local, state, tribal, territorial, and federal laws, statutes, and regulations and that these methods are not based on misleading information-gathering practices.

F.6 The FUSION CENTER will not directly or indirectly receive, seek, accept, or retain information from:

F.6.1. An individual who or nongovernmental entity that may or may not receive a fee or benefit for providing the information, except as expressly authorized by law or center policy.

F.6.2. An individual who or information provider that is legally prohibited from obtaining or disclosing the information.

F.7 Information-gathering and investigative techniques used by the FUSION CENTER will and those used by originating agencies should be the least intrusive means necessary in the particular circumstances to gather information it is authorized to seek or retain.

G. INFORMATION QUALITY ASSURANCE

G.1 The FUSION CENTER is responsible for the quality and accuracy of the data accessed by the Center. Inaccurate personal information can have a damaging impact on the person concerned and on the integrity and functional value of the FUSION CENTER. In order to maintain the integrity of the FUSION CENTER, any information obtained through the center will be independently verified with the original source from which the data was extrapolated and subjected to review, analysis, and scrutiny to derive its meaning and value, and that the appropriate metadata is affixed to each *Record*

delineating the date of receipt, nature, category, and classification before the information is qualified for use. Additionally, information will only be merged with other information about the same individual or organization when the applicable standard has been met as described in Section I, Merging Records. *Participating 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.

G.2 Any *Participating Agency* submitting information to the FUSION CENTER remains the owner of that information and is responsible for its accuracy and must ensure the quality of each *Record* submitted by the agency and the quality of the information supporting that *Record*. After submitting information about a suspected individual criminal member to the FUSION CENTER, that agency must maintain all supporting documentation for as long as: the *Record* is retained; or a legal challenge to the *Record* is pending.

G.3 The FUSION CENTER will reevaluate *Record*s whenever new information is gathered or received on an existing intelligence record. The nature, classification, categorization, and other metadata will be reevaluated and modified to reflect the impact the new information may have on the confidence and metadata assigned to the *Record*.

G.4 At the time of retention in the system, the FUSION CENTER will label information regarding its level of quality (accuracy, completeness, currency, and confidence [source reliability and content validity]). The FUSION CENTER will also conduct periodic data quality reviews of information it originates and receives, and will make every reasonable effort to ensure that the information will be corrected, deleted from the system, or not used when the center identifies information that is erroneous, misleading, obsolete, or otherwise unreliable; the center did not have authority to gather the information or to provide the information to another agency; or the center used prohibited means to gather the information (except when the center's information source did not act as the agent of the center in gathering the information).

G.5 The FUSION CENTER will evaluate all data, including, but not limited to the FUSION CENTER data, and any *Participating Agency* data, at a minimum of every five years from the date of receipt, for determination of relevance and continuing criminal predicate for retention. *Record*s that fail to meet these evaluation criteria will be purged. The Fusion Center will keep no record of any individual *Record*s purged but will identify the number of *Record*s purged. The FUSION CENTER will make every reasonable effort to ensure that information will be corrected, deleted from the system, or not used when it learns that the information lacks adequate context or is erroneous, misleading, obsolete, or otherwise unreliable.

G.6 The FUSION CENTER will use written or electronic notification to inform the originating entity, *Participating Agency*, another agency, or a database when information previously obtained or provided by the entity is determined to be erroneous, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the rights of the individual may be affected.

G.7 The FUSION CENTER will use written or electronic notification to inform recipient agencies when information previously provided to the recipient agency is deleted or changed by the center because the information is determined to be erroneous, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the rights of the individual may be affected.

H. COLLATION AND ANALYSIS

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

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

H.3 Information acquired or received by the FUSION CENTER or accessed from other sources is analyzed according to priorities and needs and will be analyzed only to:

H.3.1. Further crime prevention (including terrorism), law enforcement, public safety, force deployment, or prosecution objectives and priorities established by the center.

H.3.2. Provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal (including terrorist) activities.

H.4 The FUSION CENTER requires that all analytical products be reviewed and approved by a supervisor or, where release is required under the Freedom of Information Act or the Texas Open Records Act, the Administrator to ensure that they provide appropriate privacy, civil rights, and civil liberties protections prior to dissemination or sharing by the center.

I. MERGING RECORDS

I.1 *Records* about an individual or organization from two or more sources will not be merged by the FUSION CENTER unless there is sufficient identifying information to reasonably conclude that the information is about the same individual or organization. The set of identifiers sufficient to allow merging will consist of all available attributes that can contribute to higher accuracy of match.

I.2 If the matching requirements are not fully met but there is an identified partial match, the information may be associated by the FUSION CENTER 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

J.1 Credentialed, role-based access criteria will be used by the FUSION CENTER, as appropriate, to control:

J.1.1. The information to which a particular group or class of users can have access based on the group or class.

J.1.2. The information a class of users can add, change, delete, or print.

J.1.3. To whom, individually, the information can be disclosed and under what circumstances.

J.2 The FUSION CENTER's policy for the dissemination of information is described and defined in Section E.11.

J.3 ISE Functional Standards for the FUSION CENTER'S SAR information sharing are described in Section E.6.10 to E.6.12.

J.4 Access to or disclosure of *Record*s retained by the FUSION CENTER 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 safety, 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.

J.5 *Participating Agencies* or other agencies external to the FUSION CENTER may not disseminate information accessed or disseminated from the center without approval from the center or other originator of the information.

J.6 Information gathered or collected and *Record*s retained by the FUSION CENTER may be accessed or disseminated for specific purposes upon request by persons authorized by law to have such access and only for those uses and purposes specified in the law.

J.7 Information gathered or collected and *Record*s retained by the FUSION CENTER 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.

J.8 Information gathered or collected and *Record*s retained by the FUSION CENTER may not be accessed or disclosed to a member of the public under certain circumstances as described and defined in Section K.1.

J.9 An audit trail will be maintained by the FUSION CENTER when it disseminates an intelligence record. An audit trail will be kept for a minimum of 3 years and will include the following information about the dissemination:

J.9.1. the suspect and personally identifying information released,

J.9.2. the date and time of the query or other related access transaction; and

J.9.3. the name of the individual and agency requesting the *Record*.

J.10 A *Participating Agency* who receives and further disseminates intelligence information will create and maintain a dissemination log. The log created by the agency must:

J.10.1. comply with the principles of 28 CFR; and

J.10.2. be maintained for as long as the information supports a current *Record*.

J.11 A *Participating Agency* will permit indirect access to an intelligence record by:

J.11.1. dissemination typically through personal intervention; and

J.11.2. using a communications network only if the network involves an encrypted radio broadcast or other reasonably secure transmission method, except in the case of an emergency, when necessary to avoid imminent danger to life or property.

J.12 There are several categories of *Record*s that will ordinarily not be provided to the public:

J.12.1. Records required to be kept confidential by law are exempted from disclosure requirements under Chapter 552, Texas Government Code.

J.12.2. Information that meets the definition of "classified information" as that term is defined in the National Security Act, Public Law 235, Section 606, and in accord with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010.

J.12.3. A record or part of a record that is confidential by law under Chapter 418, Texas Government Code, including information the public disclosure of which would have a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack or other criminal activity. This may include, but is not limited to a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism or an act of agricultural terrorism, vulnerability assessments, risk planning documents, needs assessments, and threat assessments.

J.12.4. Investigatory records of law enforcement agencies that are exempted from disclosure requirements under Texas Government Code § 552.108. However, certain law enforcement records must be made available under Chapter 552, Texas Government Code.

J.12.5. Federal records, protected under federal law, which may include records exempt from disclosure under the Freedom of Information Act (FOIA) that have been provided by the Federal government.

J.12.6. Protected federal, state, local or tribal records, which may include records originated and controlled by another agency that cannot be shared without permission, unless it is required to be disclosed under the Texas Public Information Act**.**

J.12.7. A violation of an authorized nondisclosure agreement between the Fusion Center and any other party.

J.13 The FUSION CENTER will archive all intelligence products that are received and then used to further refine FUSION CENTER intelligence or are quoted or used to support disseminated intelligence products that are created. All FUSION CENTER analytical products that use another agency intelligence product information or analysis will be noted in the release of the FUSION CENTER product along with the value assigned by that product to the information. The FUSION CENTER will archive all intelligence products that are created and disseminated from the FUSION CENTER.

J.14 Information gathered and records retained by the FUSION CENTER will not be:

J.14.1. sold, published, exchanged, or disclosed for commercial purposes;

J.14.2. disclosed or published without prior notice to the originating agency that such information is subject to disclosure or publication, unless disclosure is agreed to as part of the normal operations of the agency; or

J.14.3. disseminated to persons not authorized to access or use the information.

J.15 The FUSION CENTER shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information unless otherwise required by law.

K. REDRESS

K.1 DISCLOSURE

K.1.1 Upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identify and subject to the conditions 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 FUSION CENTER.

K.1.2 The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information, pursuant to Texas Government Code Chapter 552 and subject to Section K.1.3. The procedure to submit a request is described in Section K.2.2.b. A record will be kept of all requests and of what information is disclosed to an individual. Furthermore, 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.

K.1.3 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 pursuant to the Texas Government Code, § 552.108;

b) disclosure would endanger the health or safety of an individual, organization, or community pursuant to Title 5 U.S.C. § 552(b)(7)(F);

c) the information is in a criminal intelligence system subject to 28 CFR § 23.20(e);

d) the information source does not reside with the center;

e) the FUSION CENTER did not originate or does not have a right to disclose the information, unless required by Texas Government Code, Chapter 552 Public Information; or,

f) other authorized basis for denial under the Texas Public Information Act.

K.1.4 If the information does not originate with the center, the center will notify the source agency of the request, and if appropriate, its determination that disclosure by the center was neither required nor appropriate under applicable law, in writing or electronically within 10 days.

K.2 CORRECTIONS

If an individual requests correction of information originating with the FUSION CENTER 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 the requests are denied in whole or in part. A record will be kept of all requests for corrections and the resulting action, if any.

K.3 APPEALS

The individual who has requested disclosure or to whom information has been disclosed will be given reasons if disclosure or requests for corrections are denied by the FUSION CENTER 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.

K.4 COMPLAINTS

K.4.1. 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, or

c) is held by the FUSION CENTER and allegedly has resulted in demonstrable harm to the complainant.

K.4.2. The center will inform the individual of the procedure for submitting and resolving such complaints. Inquiries and complaints about privacy, civil rights and civil liberties will be received by the center's Privacy Officer or designee at the following address: pd_fusion@elpasotexas.gov. The Privacy Officer or designee will acknowledge the complaint and state that it will be reviewed but will not confirm the existence or nonexistence of the information to the complainant unless otherwise required by law. If the information did not originate with the center, the Privacy Officer or designee will notify the originating agency in writing or electronically within 10 days and, upon request, assist such agency to correct any identified data or 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 or 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.

K.4.3. To delineate protected information shared through the ISE from other data, the FUSION CENTER maintains records of agencies sharing terrorism-

related information and employs system mechanisms to identify the originating agency when the information is shared.

K.4.4. The FUSION CENTER'S Administrator is designated as the center's Privacy Officer, including ISE, as defined in Section C.4.

L. SECURITY SAFEGUARDS

L.1 The FUSION CENTER's Administrator is designated and trained to serve as the center's Security Officer.

L.2 The FUSION CENTER will operate in a secure facility protected from external intrusion. The FUSION CENTER will utilize secure internal and external safeguards against network intrusions. Access to the FUSION CENTER's databases from outside the facility will be allowed only over secure networks.

L.3 The FUSION CENTER 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..

L.4 The FUSION CENTER will store and limit access to information in a manner such that it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions.

L.5 The FUSION CENTER will limit data access to those individuals who have been selected, approved, and trained accordingly. Access to information contained within the FUSION CENTER and its systems will be granted only to law enforcement agency personnel who have been screened with a state and national fingerprint-based background check, as well as any additional background screening processes using procedures and standards established by the FUSION CENTER GOVERNANCE BOARD. Each individual user must complete an Individual User Agreement in conjunction with training.

L.6 Once the requirements described and defined in Section L.5 have been satisfied and the completion of the City of El Paso computer security request form, the Administrator may accept a user and provide a role-based user ID and password necessary for the individual to access any intelligence system as an Authorized User through an authorized computer terminal.

L.7 Intelligence system(s) passwords will periodically expire and the Authorized User must then create a new password.

L.8 Access to the FUSION CENTER's data repositories from outside the facility will only be allowed over secure networks, encrypted radio broadcast or other reasonably secure transmission method, except in the case of an emergency, when necessary to avoid imminent danger to life or property.

L.9 The FUSION CENTER will utilize watch logs to maintain audit trails of requested and disseminated information and will identify the user initiating the query.

L.10 The FUSION CENTER will maintain watch logs of all access through portals and usage of the center's data repositories.

L.11 The FUSION CENTER will maintain watch logs of the physical access through the center's access control system.

L.12 The FUSION CENTER will conduct periodic audits of the watch logs to ensure that security and the integrity of the data and facility is maintained.

L.13 To prevent public records disclosure, risk and vulnerability assessments will not be stored with publicly available data.

L.14 The FUSION CENTER and any *Participating Agency* shall comply with the security provisions of the Criminal Justice Information Services (CJIS) Security Policy. The agency shall provide for reasonable:

L.14.1 physical security, including a secure area for placement of each item of equipment to preclude physical access by other than authorized personnel and to control visitor access;

L.14.2 operational security, including equipment operated to preclude system access by other than authorized personnel or for other than authorized purposes and to change system access identifiers for terminated or reassigned personnel; and

L.14.3 personnel security, including access allowed only to:

a) law enforcement, military acting under Title 32 or criminal justice personnel; or

b) technical or maintenance personnel who have been subject to character or security clearance.

L.15 Compromising a user ID or password is a serious violation of system security.

L.16 The procedure for data security breach notification is described and defined in Section N.2.9.

L.17 A Participating Agency must notify the Administrator when an individual is terminated or reassigned and is, therefore, no longer eligible to continue as an authorized user; comply with FUSION CENTER's quality control, inspection, audit, and validation procedures.

M. INFORMATION RETENTION AND DESTRUCTION

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

M.2. When information has no further value or meets the criteria for removal according to the FUSION CENTER's retention and destruction policy as provided by Texas Government Code Chapter 441, it will be purged, destroyed, and deleted or returned to the submitting (originating) agency.

M.3. The 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.

M.4. No approval will be required from the originating agency before information held by the 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.

M.5. Notification of proposed destruction or return of *Record*s may or may not be provided to the originating agency by the FUSION CENTER, depending on the relevance of the information and any agreement with the originating agency.

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

N. ACCOUNTABILITY AND ENFORCEMENT

N.1 INFORMATION SYSTEM TRANSPARENCY

N.1.1 The FUSION CENTER will be open with the public in regard to information and intelligence collection practices.

N.1.2 The FUSION CENTER will provide a printed or electronic copy of this policy upon request by any person, corporation, or organization.

N.1.3 The FUSION CENTER will post a copy of this policy on the center's website at www.eppd.com/fusion.

N.1.4 The FUSION CENTER'S point of contact for inquires and complaints is designated in Section K.2.2.

N.2 ACCOUNTABILITY

N.2.1 The FUSION CENTER will maintain watch logs of all access as described and defined in Section L.9.

N.2.2 The FUSION CENTER 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 of all systems as described and defined in Section L. These audits will be mandated at least annually and a record of the audits and requests for information for specific purposes and of what information is disseminated to each person in response to the request will be maintained for a minimum of 3 years by the Administrator of the center.

N.2.3 The FUSION CENTER will undergo an annual audit and inspection of the information contained in the FUSION CENTER's criminal intelligence systems and its compliance with this Privacy Policy. The audit will be conducted by the FUSION CENTER Administrator. The Administrator has the option of conducting a random audit, without announcement, at any time and without prior notice to staff of the center. The audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the center's information and intelligence system(s). The FUSION CENTER will undergo an annual audit as prescribed by the Texas Fusion Center Policy Council (TFCPC) pursuant to the Texas Government Code Chapter 421.

N.2.4 Each *Participating Agency* is subject to a regular annual audit by a FUSION CENTER representative of submitted data and compliance with the Privacy Policy. The FUSION CENTER may specially inquire into any demonstrated failure to comply with these policies and procedures.

N.2.5 The FUSION CENTER will make at least an annual report of any known or reported breaches of security of improper handling or loss of Personal Identifying Information. This report will not identify affected persons or their personal information but will identify incidents and corrective measures taken.

N.2.6 A *Participating Agency* has an affirmative responsibility to immediately report the loss or mishandling of any personal or sensitive information to the Commander of the FUSION CENTER, or in the Commander's absence the Administrator of the FUSION CENTER.

N.2.7 The FUSION CENTER'S personnel or other authorized users shall report errors and violations or suspected violations of FUSION CENTER'S policies relating to protected information to the FUSION CENTER Commander.

N.2.8 The FUSION CENTER requires all personnel to agree to comply with the provision of this policy in writing, as described and defined in Section B.1.4.

N.2.9 The FUSION CENTER will follow the data breach notification specified in Texas Business and Commerce Code Section 521.053, to the extent that it applies.

N.2.10 The FUSION CENTER Privacy Officer will review and update the provisions protecting privacy, civil rights, and civil liberties contained in this policy annually and will recommend appropriate changes in response to changes in applicable law, technology, the purpose and use of the information systems, and public expectations. The Privacy Officer will recommend these changes to the FUSION CENTER Commander, who will update and forward this policy for review as described and defined in Section C.2.

N.3 ENFORCEMENT

N.3.1 If an authorized user or *Participating Agency* materially violates any term of its User Agreement or is found to be in noncompliance with the provisions of this policy and procedures, the authorized user or agency risks suspension of its access to intelligence information.

N.3.2 A suspension may occur immediately and without prior notice. Suspension may be followed by termination if deemed necessary by the Administrator.

N.3.3 The Administrator shall send to the *Participating Agency* a notice within 10 working days describing:

b) the date the Administrator has suspended or proposes to terminate service;

c) the alleged violation of the User Agreement; and,

d) whether the alleged violation is criminal or under investigation.

N.3.4 If the FUSION CENTER Commander or Administrator determines the alleged violation to be criminal in nature, an investigation shall be initiated, the results of which shall be forwarded to the appropriate authority for criminal prosecution.

N.3.5 If the authorized user is from an agency external to the FUSION CENTER, request that the relevant agency, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions.

N.3.6 The FUSION CENTER reserves the right to restrict the qualifications and number of personnel having access to center information to any participating agency or participating agency personnel violating the FUSION CENTER's privacy policy.

O. **TRAINING**

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

O.1.1 all personnel assigned to the center; and,

O.1.2 staff in other public agencies or private contractors providing services to the center.

O.2 The FUSION CENTER 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 (ISE).

O.3 The FUSION CENTER's privacy policy training program will cover:

O.3.1 purposes of the privacy, civil rights, and civil liberties protection policy;

O.3.2 substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the center;

O.3.3 originating and *Participating Agency* responsibilities and obligations under applicable law and policy;

O.3.4 how to implement the policy in the day-to-day work of the user, whether a paper or systems user;

O.3.5 the impact of improper activities associated with infractions within or through the agency;

O.3.6 mechanisms for reporting violations of center privacy protection policies and procedures; and,

O.3.7 the nature and possible penalties for policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.

O.4 The FUSION CENTER will provide training for all *Authorized Users* granted *Direct Access* to any intelligence systems in the operational aspects of the systems.

O.5 The FUSION CENTER may require additional training for any user or *Participating Agency* under State training requirements or law.

P. RESERVATION AND USER AGREEMENT

P.1 Agencies may choose to exercise a written User Agreement to further define roles and responsibilities to ensure compliance with this Privacy Policy and addendum. Nothing in this Privacy Policy may be used to limit the responsibility of the FUSION CENTER in pursuing efforts to satisfy its other legal rights, privileges or obligations.

Appendix A: Terms and Definitions

In this PRIVACY POLICY:

1. "**Administration of criminal justice**" means the performance of any of the following activities: detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of a criminal offender. The term includes criminal identification activities and the collection, storage, and dissemination of criminal record information.

2. "**Administrator**" means the individual appointed by the FUSION CENTER's Commander as the system administrator for intelligence systems or another individual designated to serve in that capacity; the Privacy Officer; and, the Security Officer for the FUSION CENTER.

3. "**Authorized user**" means an individual designated by an agency head and authorized by the El Paso Police Dept. Fusion Center Administrator for direct access to intelligence systems.

4. "**Direct access**" means the action of an individual authorized user to gain direct computer access to intelligence system.

5. "**Lead Agency**" means the El Paso Police Department.

6. "**CCP** " means the Texas Code of Criminal Procedure.

7. "**28 CFR**" means Title 28, Code of Federal Regulations, Part 23.1 et seq., as promulgated by the U.S. Department of Justice, Office of Justice Programs.

8. "**Criminal intelligence**" means information, material, photographs, or data that has been evaluated to determine that it is relevant to the identification of an individual or an organization for which a proper criminal predicate exists.

9. "**Criminal justice agency**" means a federal, state, or local entity that is engaged in the administration of criminal justice under a statute or executive order and that allocates a substantial part of its annual budget to the administration of criminal justice.

10. "**Criminal predicate**" means reasonable suspicion or is defined or established when information exists that substantiates sufficient facts to give a trained law enforcement or criminal investigative agency, officer, investigator or assigned employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise.

11. "**Criminal street gang**" or "**gang**" means three or more individuals having a common identifying sign or symbol or an identifiable leadership who continuously or regularly associate in the commission of identifiable criminal activities.

12. "**Criminal street gang member**" or "**gang member**" means an individual who has been identified as a member of a criminal gang through documentation supported by 28 CFR Part 23 standards.

13. "**Fair Information Principles**" are contained within the Organization for Economic Co-operation and Development's (OECD) *Guidelines on the Protection of Privacy and Transborder Flow of Personal Data.* These were developed around commercial transactions and the transborder exchange of information; however, they do provide a straightforward description of underlying privacy and information exchange principles and provide a simple framework for the legal analysis that needs to be done with regard to privacy in integrated justice systems. Some of the individual principles may not apply in all instances of an integrated justice system. The eight FIPs are: Collection Limitation Principle, Data Quality Principle, Purpose Specification Principle, Use Limitation Principle, Security Safeguards Principle, Openness Principle, Individual Participation Principle, and Accountability Principle.

14. "**Fusion Center Supervisor"** means a person appointed by the El Paso Police Department with the authority to plan, organize, direct and control day-to-day field or station activities of an assigned uniformed officer, detective or police support unit on a designated shift. Includes the ability to enforce rules, regulations, policies and procedures associated with the governance of the Fusion Center

15. "**Indirect access**" means the action of an individual, who is not an authorized user, to gain indirect access to intelligence systems through an A*uthorized User* based on a *right to know and/or a need to know*.

16. "**Information quality**" means the validity, accuracy, timeliness, completeness, relevancy, importance, and reliability of information supporting an intelligence system record.

17. "**Intelligence Information Validity**" is that evaluation assessed by an *Authorized User* or other trained person regarding the validity of the information or record submitted as to the information accuracy or truthfulness and is assigned as "*Confirmed*", "*Probable*", "*Doubtful*" and "*Can Not Be Judged*", as defined by and consistent with 28 CFR Part 23 definitions.

18. "**Intelligence Source Reliability**" is that evaluation assessed by an *Authorized User* or trained person regarding the consistency of the source in providing intelligence information and is assigned as "*Reliable*", "*Usually Reliable*", "*Unreliable*" and "*Unknown*" as defined by and consistent with 28 CFR Part 23 definitions.

19. "**Intelligence project**" has the meaning given that term by 28 CFR. The term includes El Paso Police Department acting through the **FUSION CENTER.**

20. "**Local entity**" means an agency or other entity of a political subdivision of the State, including a city or county. The term includes a task force, law enforcement agency of a school district or institution of higher education, whether public or private, or other local entity that is engaged in the administration of criminal justice under a statute or executive order.

21. "**Need to know**" means the necessity to obtain or receive criminal intelligence information in the performance of an official duty or responsibility for a criminal justice agency. However, the ***Need to Know*** criteria should not be weighed solely as a method to prevent dissemination but rather as an affirmative responsibility to share information where such dissemination may improve public safety or an individual officer safety or overall effectiveness of a law enforcement agency. The **Need to Know** provision shall not prohibit the release of information where there is an imminent threat to life that mandates the release of information.

22. "**Participating Agency**" or **"Participating Agencies"** means a criminal justice agency that has entered into a User Agreement.

23. **"Personally Identifiable Information"** means one or more pieces of information, such as personal characteristics and unique identifiers, that when considered together or when considered in the context of how it is present or how it is gathered is sufficient to specify a unique individual.

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

25. "**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 Texas 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 and ordinances. Protection may also be extended to organizations by **FUSION CENTER** policy or state, local, or tribal law.

26. "**Record**" means information accepted by the Lead Agency or **FUSION CENTER** for storage and retention in an intelligence system.

27. "**Record quality**" means that the data format of any record meets all Quality Control provisions and system edits under these policies and procedures.

28. "**Reasonable Suspicion**" or criminal predicate is defined or established when information exists that substantiates sufficient facts to give a trained law enforcement or criminal investigative agency, officer, investigator or assigned employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise

29. "**Right to know**" means the legal authority to obtain or receive criminal intelligence information under a court order, statute, or decisional law or Lead Agency policy.

30. "**Right to Know**" shall also apply to any submitting agency as the owner of applicable submitted information permitting their access to and mandating their responsibility for applicable submitted information.

31 "**Suspicious Activity Report**" (SAR) is the 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.

32. "**Tips and Leads" Information or Data** is 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.

33. "**User Agreement**" means an agreement or written understanding executed under these policies and procedures between the El Paso Police Department, its FUSION CENTER and a *Participating Agency*.

34. "**Validation**" means the determination of the continuing viability, accuracy, and relevancy of the criminal intelligence information supporting an intelligence record as defined by 28 CFR standards for *Reasonable Suspicion*. The term includes the record review, retention, or purge and removal processes required under either 28 CFR or CCP.

Appendix B: State and Federal Law Relevant to Seeking, Retaining, and Disseminating Justice Information

Following is a partial listing of laws arranged in alphabetical order by popular name.

State Laws

Texas Constitution

Texas Code of Criminal Procedure Chapter 61 and amendments contained in Senate Bill 418 81st Legislature, regarding Gang Intelligence and 28 CFR standards

Chapter 421 of the Texas Government Code, regarding the Department of Public Safety and the collection of terrorist and Homeland Security information

Chapter 552 of the Texas Government Code, regarding open government

Texas Business and Commerce Code Section 521.053, regarding data breach notification

Federal Laws

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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