

Colorado Information Analysis Center

Privacy Policy



CIAC

**Colorado Information
Analysis Center**

Department of Public Safety

January 2019

Colorado Information Analysis Center Privacy Policy

**Colorado Information Analysis Center
Division of Homeland Security and Emergency Management
Colorado Department of Public Safety**

2010-Version 3

January 2019

Table of Contents

- I. PURPOSE STATEMENT 4
- II. POLICY APPLICABILITY AND LEGAL COMPLIANCE 5
- III. GOVERNANCE AND OVERSIGHT 5
- IV. INFORMATION 6
- V. ACQUIRING AND RECEIVING INFORMATION 8
- VI. INFORMATION QUALITY ASSURANCE 9
- VII. COLLATION AND ANALYSIS 10
- VIII. MERGING RECORDS..... 10
- IX. SHARING AND DISCLOSURE 11
- X. REDRESS..... 12
 - 1. Disclosure..... 12
 - 2. CORRECTIONS 13
 - 3. APPEALS 13
 - 4. COMPLAINTS..... 14
- XI. SECURITY SAFEGUARDS..... 14
- XII. INFORMATION RETENTION AND DESTRUCTION 15
- XIII. ACCOUNTABILITY AND ENFORCEMENT 15
 - 1. Information System Transparency 15
 - 2. Accountability 16
 - 3. Enforcement 16
- XIV. TRAINING 17

Colorado Information Analysis Center Privacy Policy

I. PURPOSE STATEMENT

The mission of the Colorado Information Analysis Center (CIAC) is to ensure a safe and secure environment for the citizens of Colorado from intentional acts of terrorism, accidental harmful events or natural disasters through the implementation of innovative prevention methods, coordinated response procedures and effective recover plans.

The CIAC is comprised of the state's fusion center, the CIAC, which is comprised of an analytical unit, Colorado State Patrol Intel Unit, and the Auto Theft Intelligence Coordination Center (ATICC).

The primary focus of the CIAC is the collection, analysis and dissemination of all hazards/all crimes intelligence including counter terrorism and providing a suspicious activity reporting (SAR) system. This is a process where information is collected, integrated, evaluated, analyzed and disseminated through established procedures for law enforcement purposes and in the interest of public safety. This is accomplished while protecting privacy and civil liberties.

The purpose of this privacy, civil rights, and civil liberties protection policy is to facilitate the CIAC and CIAC users' compliance with applicable federal, state, local, and tribal law and assist the Center and its users in:

- Protecting individual privacy, civil rights, civil liberties, and other protected interests
- Increasing public safety and improving national security
- Minimizing the threat and risk of injury to specific individuals
- Minimizing the threat and risk of physical or financial injury to law enforcement and others responsible for public protection, safety, or health
- Minimizing the threat and risk of damage to real or personal property
- Protecting the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information
- Minimizing reluctance of individuals or groups to use or cooperate with the justice system
- Supporting the role of the justice system in society
- Promoting governmental legitimacy and accountability
- Not unduly burdening the ongoing business of the justice system
- Making the most effective use of public resources allocated to public safety agencies

This policy is intended to be a part of the Center's overall governance architecture which include; the Information Sharing Environment Guidelines (Appendix B), the 28 CFR Part 23 Flow Chart (Appendix C), and the Center's Standard Operating Procedures and Product Dissemination Guidelines (Appendix D).

II. POLICY APPLICABILITY AND LEGAL COMPLIANCE

All CIAC personnel, including permanently assigned part-time personnel, voluntary unpaid interns, participating agency personnel, personnel providing information technology services to the Center and other authorized users will comply with the Center's privacy policy. This policy applies to information the Center gathers or collects, receives, maintains, stores, accesses, discloses, or disseminates to Center personnel, governmental agencies, other fusion centers, and participating justice and public safety agencies, as well as to private contractors, private entities, and the general public.

The CIAC will provide a printed or electronic copy of this policy to all Center and non-center personnel who provide services and to participating agencies and individual users and will require both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and the applicable provisions it contains. The policy is also available on the Center's public website.

All CIAC personnel, participating agency personnel, personnel providing information technology services to the Center, private contractors, agencies from which Center information originates, and other authorized users will comply with applicable law protecting privacy, civil rights, and civil liberties, including, but not limited to the U.S. Constitution and the Colorado Constitution, 28 CFR Part 23, the Fair Information Practices as outlined by the National Criminal Justice Association (NCJA), Colorado Title 24, Colorado Open Records Act Part 2, and any additional applicable state or federal law.

The CIAC has adopted internal operating policies that are in compliance with applicable law protecting privacy, civil rights, and civil liberties, including, but not limited to 28 CFR Part 23, the Fair Information Practices as outlined by the National Criminal Justice Association (NCJA) and any additional applicable state or federal law listed above.

III. GOVERNANCE AND OVERSIGHT

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

The CIAC is guided by the Director of the Division of Homeland Security and emergency Management within the Colorado Department of Public Safety to ensure that privacy and civil rights are protected as provided in this policy and by the Center's information gathering and collection, retention, and dissemination processes and procedures. The Director will annually review and update the policy in response to changes in law and implementation experience, including the results of audits and inspections.

The CIAC's privacy committee is guided by the CIAC Director who designates a Center "Privacy Officer." The Privacy Officer receives reports regarding alleged errors and violations of the provisions of this policy, receives and coordinates complaint resolution under the Center's redress policy as discussed in Section X, and serves as the liaison for the Information Sharing Environment (ISE), ensuring that privacy protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy enhancing technologies.

The Privacy Officer can be contacted at cdps_ciac@state.co.us or at the following address:

Colorado Information Analysis Center
690 Kipling St. Suite 2100
Lakewood, CO 80215

The CIAC's Privacy Officer ensures that enforcement procedures and sanctions outlined in Section XIII are adequate and enforced.

IV. INFORMATION

The CIAC will collect, gather, retain, or disseminate information that:

- Is based on a possible threat to public safety or the enforcement of the criminal law; or
- Is based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal conduct (including terrorism) or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal conduct (including terrorism) or activity; or
- Is relevant to the investigation and prosecution of suspected criminal activities (including terrorism); the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime; or
- Is useful in crime analysis or in the administration of criminal justice and public safety (including topical searches); and
- The source of the information is reliable and verifiable or limitations on the quality of the information are identified; and
- The information was collected in a fair and lawful manner with the knowledge and consent of the individual, if appropriate.

The Center may retain protected information that is based on a level of suspicion that is less than "reasonable suspicion," such as tips and leads or suspicious activity report (SAR) information, subject to the policies and procedures specified in this policy.

The CIAC will not seek or retain, and information originating agencies will 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. The CIAC applies labels to Center-originated information (or ensures that the originating agency has applied labels) to indicate to the accessing authorized user that:

- The information is protected information as defined by the ISE Privacy Guidelines and, to the extent expressly provided in this policy, includes organizational entities.
- The information is subject to Title 24 of the Colorado revised statute that restricts access, use, or disclosure.

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

- Whether the information consists of tips and leads data, suspicious activity reports, criminal history, intelligence information, case records, conditions of supervision, case progress, or other information category.
- The nature of the source as it affects veracity (for example, anonymous tip, trained interviewer or investigator, public record, private sector).
- The reliability of the source (for example, reliable, usually reliable, unreliable, unknown).
- The validity of the content (for example, confirmed, probable, doubtful, cannot be judged).

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

- Protect an individual's right of privacy, civil rights and civil liberties.
- Protect confidential sources and police undercover techniques and methods.
- Not interfere with or compromise pending criminal investigations.
- 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.

The labels assigned to existing information under this Information Policy (see Section IV) will be reevaluated whenever:

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

CIAC personnel are required to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of tips and leads and SAR information. CIAC personnel will:

- Prior to allowing access to or dissemination of the information, ensure that attempts to validate or refute the information have taken place and that the information has been assessed for sensitivity and confidence by subjecting it to an evaluation or screening process to determine its credibility and value and categorize the information as unsubstantiated or uncorroborated if attempts to validate or determine the reliability of the information have been unsuccessful. The Center will use a standard reporting format and data collection codes for SAR information.
- Store the information using the same storage method used for data that rises to the level of reasonable suspicion and which includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information.
- Allow access to or disseminate the information using the same access or dissemination standard that is used for data that rises to the level of reasonable suspicion (for example, "need-to-know" and "right-to-know" access or dissemination for personally identifiable information).
- Regularly provide access 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 if the information to any agency, entity, individual, or the public when credible information indicates potential imminent danger to life or property.
- Retain information for 30 days in order to work a non-validated tip, lead, or SAR information to determine its credibility and value or assign a "disposition" label (for example, undetermined or

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

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

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

The CIAC will identify and review protected information that may be accessed from or disseminated by the Center prior to sharing that information through the ISE. 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.

The CIAC requires certain basic descriptive information to the extent reasonably possible be entered and associated with data for which there are special laws, rules, or policies regarding access, use, and disclosure. The types of information include:

- The name of the originating center, department or agency, component, and subcomponent
- The name of the center's justice information system from which the information is disseminated
- The date the information was collected and, where feasible, the date its accuracy was last verified
- The title and contact information for the person to whom questions regarding the information should be directed

The CIAC will attach specific labels and descriptive metadata to information that will be used, accessed, or disseminated to clearly indicate any legal restrictions on information sharing based on information sensitivity or classification.

The CIAC will keep a record of the source of all information sought and collected by the Center.

V. ACQUIRING AND RECEIVING INFORMATION

Information gathering, acquisition, and investigative techniques used by the CIAC and information-originating agencies will remain in compliance with and will adhere to applicable law and guidance, including, but not limited to:

- 28 CFR Part 23 regarding criminal intelligence information
- Criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) *National Criminal Intelligence Sharing Plan* (NCISP)
- Constitutional provisions, the Code of Federal Regulations 28 part 23, Colorado Title 24, the criminal intelligence collection guidelines established under the National Criminal Intelligence

Sharing Plan (NCISP), and administrative rules, as well as regulations and policies that apply to multijurisdictional intelligence and information databases.

The CIAC'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 or criminal nexus. Law enforcement officers and appropriate Center and participating agency staff will be trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism.

The CIAC'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.

Information-gathering and investigative techniques used by the CIAC will be conducted in the least intrusive means necessary and in accordance with legal authority and this policy.

External agencies that access the CIAC'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.

The CIAC 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.

The CIAC will not knowingly receive, seek, accept, or retain information from:

- An individual or nongovernmental entity that may or may not receive a fee or benefit for providing unlawfully obtained information.
- An individual or information provider that is legally prohibited from obtaining or disclosing the information.

VI. INFORMATION QUALITY ASSURANCE

The CIAC will make every reasonable effort to ensure that information sought or retained is: derived from dependable and trustworthy sources; accurate; current; complete, including the relevant context in which it was sought or received and other related information; and merged with other information about the same individual or organization only when the applicable standard (see Section VIII) has been met.

At the time of retention in the system, the information will be labeled regarding its level of quality (accuracy, completeness, currency, verifiability, and reliability). The CIAC examines, in a timely manner, alleged errors and deficiencies (or refers them to the originating agency) and corrects, deletes, or refrains from using protected information found to be erroneous or deficient.

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

The CIAC will conduct periodic data quality reviews of information it originates and retains and make every reasonable effort to ensure that the information will be corrected, deleted from the system, or not used when the Center identifies information that is erroneous, misleading, obsolete, or otherwise unreliable; or 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).

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

The CIAC 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.

VII. COLLATION AND ANALYSIS

Information acquired or received by the CIAC 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.

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

Information acquired or received by the CIAC or accessed from other sources is analyzed according to priorities and needs and will be analyzed only to:

- Further crime prevention (including terrorism), law enforcement, public safety, or prosecution objectives and priorities established by the Center.
- Provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal (including terrorism) activities.

The CIAC requires that all analytical products be reviewed and approved by the Privacy Officer or a properly trained designee to ensure that they provide appropriate privacy, civil rights, and civil liberties protections prior to dissemination or sharing by the Center.

VIII. MERGING RECORDS

Records about an individual or organization from two or more sources will not be merged by the CIAC unless there is sufficient identifying information to reasonably conclude that the information is about

the same individual or organization. The set of identifiers sufficient to allow merging will consist of all available attributes that can contribute to a higher accuracy of match.

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

IX. SHARING AND DISCLOSURE

Credentialed, role-based access criteria will be used by the CIAC, as appropriate, to control:

- The information to which a particular group or class of users can have access based on the group or class.
- The information a class of users can add, change, delete, or print.
- To whom, individually, the information can be disclosed and under what circumstances.

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

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

Agencies external to the CIAC may not disseminate information outside of the provided handling provisions without approval from the Center or the originator of the information.

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

Information gathered or collected and records retained by the CIAC may be accessed or disseminated **for specific purposes** upon request by persons authorized by law to have such access and only for those uses and purposes specified in the law. An audit trail sufficient to allow the identification of each individual who requested, accessed, or received information retained by the Center, the nature of the information requested, accessed, or received, and the specific purpose will be kept for 5 years by the Center.

Information gathered or collected and records retained by the CIAC may be accessed or disclosed **to a member of the public** only if the information is defined by law to be a public record or otherwise

appropriate for release to further the Center's mission and is not exempt from disclosure by law. Such information may be disclosed only in accordance with the law and procedures applicable to the Center for this type of information. An audit trail sufficient to allow the identification of each individual member of the public who accessed or received information retained by the Center and the nature of the information accessed will be kept by the center indefinitely.

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

- Sold, published, exchanged, or disclosed for commercial purposes.
- Disclosed or published without prior notice to the originating agency that such information is subject to disclosure or publication, unless disclosure is agreed to as part of the normal operations of the agency.
- Disseminated to persons not authorized to access or use the information.

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

- Records required to be kept confidential by law are exempted from disclosure requirements under Colorado Open Records Act 24-72-204, C.R.S..
- Information that meets the definition of "classified information" as that term is defined in the National Security Act, Public Law 235, Section 606.
- Investigatory records of law enforcement agencies that are exempted from disclosure requirements under Colorado Open Records Act, Part 2 24-72-204, C.R.S.. However, certain law enforcement records must be made available for inspection and copying under Colorado Open Records Act, Part 3 24-72-204, C.R.S..
- A record or part of a record the public disclosure of which would have a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack is exempted from disclosure requirements under Colorado Open Records Act, Part 2 C.R.S. 24-72-204. This includes a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism under Colorado Open Records Act, 24-72-204, C.R.S. or an act of agricultural terrorism under Colorado Open Records Act, Part 2 24-72-204, C.R.S. vulnerability assessments, risk planning documents, needs assessments, and threat assessments.
- Protected federal, state, local, or tribal records, which may include records originated and controlled by another agency that cannot, under 24-72-204, C.R.S. be shared without permission.
- A violation of an authorized nondisclosure agreement under 24-72-204, C.R.S..

The CIAC 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.

X. REDRESS

1. Disclosure

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 the individual that has been gathered and retained by the CIAC. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information (correction). The Center's

response to the request for information will be made within a reasonable time and in a form that is readily intelligible to the individual. A record will be kept of all requests and of what information is disclosed to an individual.

The existence, content, and source of the information will not be made available by the CIAC to an individual when the information is protected by Part 2 of the Colorado Open Record Act and:

- Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution
- Disclosure would endanger the health or safety of an individual, organization, or community
- The information is in a criminal intelligence information system subject to 28 CFR Part 23 (See Appendix C)
- The information source does not reside with the Center
- The Center did not originate and does not have a right to disclose the information
- Other authorized basis for denial

If the information does not originate with the Center, the requestor will be referred to the originating agency, if appropriate or required, or the Center will notify the source agency of the request and its determination that disclosure by the Center or referral of the requestor to the source agency was neither required nor appropriate under applicable law.

2. Corrections

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

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 CIAC. The individual will also be informed of the procedure for appeal when the Center 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.

- On the ground that disclosure would be contrary to the public interest, and unless otherwise provided by law, the custodian may deny access to records of investigations conducted by or of intelligence information or security procedures of criminal justice investigatory files compiled for any other law enforcement purpose.
- If the custodian denies access to any criminal justice record, the applicant may request a written statement of the grounds for the denial. The statement shall be provided to the applicant within seventy-two hours, shall cite the law or regulation under which access is denied or the general nature of the public interest to be protected by the denial, and shall be furnished to the applicant.
- Any person denied access to inspect any criminal justice record may apply to the Director of the Colorado Department of Public Safety.

4. Complaints

If an individual has a complaint with regard to the accuracy or completeness of protected information that:

- a) Is exempt from disclosure,
- b) Has been or may be shared through the ISE,
- c) Is held by the CIAC and allegedly has resulted in the demonstrable harm to the complainant

The Center will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the CIAC's Privacy Officer at cdps_ciac@state.co.us or at the following address:

Colorado Information Analysis Center
690 Kipling St. Suite 2100
Lakewood, CO 80215

The Privacy Officer will acknowledge the complaint and state that it will be reviewed but will not confirm the existence or nonexistence of the information to the complainant unless otherwise required by law. If the information did not originate with the Center, the Privacy Officer will notify the originating agency in writing or electronically within 10 days and, upon request, assist such agency to correct any identified data/record deficiencies, purge the information, or verify that the record is accurate. All information held by the Center that is the subject of a complaint will be reviewed within 30 days and confirmed or corrected/purged if determined to be inaccurate, 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 indefinitely by the Center of all complaints and the resulting action taken in response to the complaint.

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

XI. SECURITY SAFEGUARDS

The CIAC Director or designee is designated and trained to serve as the Center's security officer.

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

The CIAC will secure tips, leads, and SAR information in a separate repository system using security procedures and policies that are the same as or similar to those used for a system that secures data rising to the level of reasonable suspicion under 28 CFR Part 23.

The CIAC will store information in a manner that ensures it cannot be added to, modified, accessed, destroyed, or purged except by authorized personnel.

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

The CIAC will utilize tracking sheets to maintain audit trails of requested and disseminated information.

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

The CIAC will follow the data breach notification guidance set forth in OMB Memorandum M-07-16.

XII. INFORMATION RETENTION AND DESTRUCTION

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

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

The CIAC 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.

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

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

XIII. ACCOUNTABILITY AND ENFORCEMENT

1. Information System Transparency

The CIAC will be open with the public in regard to information and intelligence collection practices. The Center's privacy policy will be provided to the public for review, made available upon request, and posted on the Center's Web site at www.dhsem.state.co.us.

The CIAC's Director or designee will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s)

maintained or accessed by the Center. The Privacy Officer can be contacted at cdps_ciac@state.co.us or at:

Colorado Information Analysis Center
690 Kipling St. Suite 2100
Lakewood, CO 80215

2. Accountability

The audit log of queries made to the CIAC will identify the user initiating the query.

The CIAC will maintain an audit trail of accessed, requested, or disseminated information. An audit trail will be kept indefinitely of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.

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

The CIAC's personnel or other authorized users shall report errors and suspected or confirmed violations of Center policies relating to protected information to the Center's Privacy Officer (see Section III).

The CIAC will annually conduct an audit and inspection of the information and intelligence contained in its information system(s). The audit will be conducted under the authority of Director of the Colorado Department of Public Safety. The Director or his designee 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 Director of the Colorado Department of Public Safety, guided by the appointed and trained Privacy Officer, will review and update the provisions protecting privacy, civil rights, and civil liberties contained in this policy annually and will make appropriate changes in response to changes in applicable law, technology, the purpose and use of the information systems, and public expectations.

3. Enforcement

If Center personnel, a participating agency, or an authorized user is found to be in noncompliance with the provisions of this policy regarding the gathering, collection, use, retention, destruction, sharing, classification, or disclosure of information, the CIAC Director will:

- Suspend or discontinue access to information by the Center personnel, the participating agency, or the authorized user.
- Suspend, demote, transfer, or terminate Center personnel, as permitted by applicable personnel policies.

- Apply administrative actions or sanctions as provided by State of Colorado Department of Public Safety rules and regulations or as provided in the Center's personnel policies.
- If the authorized user is from an agency external to the Center, request that the relevant agency, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions.
- Refer the matter to appropriate authorities for criminal prosecution, as necessary, to implement the purposes of the policy.

The CIAC reserves the right to restrict the qualifications and number of personnel having access to Center information and to suspend or withhold service and deny access to any participating agency or participating agency personnel violating the Center's privacy policy.

XIV. TRAINING

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

- All permanent, part-time, and unpaid volunteer personnel assigned to the Center.
- Personnel providing information technology services to the Center.
- Staff in other public agencies providing services to the Center.
- Members of the public, individually or in groups, upon request.

The CIAC 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 ISE.

The CIAC's privacy policy training program will cover:

- Purposes of the privacy, civil rights, and civil liberties protection policy.
- Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the Center
- Originating and participating agency responsibilities and obligations under applicable law and policy.
- How to implement the policy in the day-to-day work of the user, whether a paper or systems user.
- The impact of improper activities associated with infractions within or through the agency.
- Mechanisms for reporting violations of Center privacy protection policies and procedures.
- The nature and possible penalties for policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.

APPENDIX A: TERMS AND DEFINITIONS

Access—Data access is being able to get to (usually having permission to use) particular data on a computer. Web access means having a connection to the World Wide Web through an access provider or an online service provider. Data access is usually specified as read-only and read/write access.

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

Access Control—The mechanisms for limiting access to certain information based on a user's identity and membership in various predefined groups. Access control can be mandatory, discretionary, or role-based.

Acquisition—The means by which an ISE participant obtains information through the exercise of its authorities; for example, through human intelligence collection or from a foreign partner. For the purposed of this definition, acquisition does not refer to the obtaining of information widely available to other ISE participants through, for example, news reports of the obtaining of information shared with them by another ISE participant who originally acquired the information.

Agency—The Colorado Information Analysis Center (CIAC) and all agencies that access, contribute, and share information in the CIAC's justice information system.

Audit Trail—A generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail—what commands were issued to the system, what records and files were accessed or modified, etc.

Audit trails are a fundamental part of computer security, used to trace (albeit usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

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

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

Biometrics—Biometrics methods can be divided into two categories: physiological and behavioral. Implementations of the former include face, eye (retina or iris), finger (fingertip, thumb, finger length or pattern), palm (print or topography), and hand geometry. The latter includes voiceprints and handwritten signatures.

Center—Refers to the CIAC and all participating agencies represented within the CIAC.

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

Civil Rights—The term “civil rights” is used to imply that the state has a role in ensuring that all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of race, religion, gender, or other characteristics unrelated to the worth of the individual. Civil rights are, therefore, obligations imposed on government to promote equality. More specifically, they are the rights to personal liberty guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments and by acts of Congress.

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

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

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

Criminal Intelligence Information—Information deemed relevant to the identification of and the criminal activity engaged in by an individual who or organization that is reasonably suspected of involvement in criminal activity. Criminal intelligence records are maintained in a criminal intelligence system per 28 CFR Part 23.

Data—Inert symbols, signs, descriptions, or measures; elements of information.

Data Breach—The unintentional release of secure information to an un-trusted environment. This may include incidents such as theft or loss of digital media such as computer tapes, hard drives, or laptop computers containing such media upon which such information is stored unencrypted; posting such information on the World Wide Web or on a computer otherwise accessible from the Internet without proper information security precautions; transfer of such information to a system that is not completely open but is not appropriately or formally accredited for security at the approved level, such as

unencrypted e-mail; or transfer of such information to the information systems of a possibly hostile agency or environment where it may be exposed to more intensive decryption techniques.

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

Disclosure—The release, transfer, provision of access to, sharing, publication, or divulging of personal information in any manner—electronic, verbal, or in writing—to an individual, agency, or organization outside the agency that collected it. Disclosure is an aspect of privacy, focusing on information which may be available only to certain people for certain purposes but which is not available to everyone.

Electronically Maintained—Information stored by a computer or on any electronic medium from which the information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, or compact disc optical media.

Electronically Transmitted—Information exchanged with a computer using electronic media, such as the movement of information from one location to another by magnetic or optical media, or transmission over the Internet, intranet, extranet, leased lines, dial-up lines, private networks, telephone voice response, or faxback systems. It does not include faxes, telephone calls, video teleconferencing, or messages left on voicemail.

Fair Information Principles—The Fair Information Principles (FIPs) are contained within the Organization for Economic Co-operation and Development's (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. These were developed around commercial transactions and the transborder exchange of information; however, they do provide a straightforward description of underlying privacy and information exchange principles and provide a simple framework for the legal analysis that needs to be done with regard to privacy in integrated justice systems. Some of the individual principles may not apply in all instances of an integrated justice system.

The eight FIPs are:

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

Firewall—A security solution that segregates one portion of a network from another portion, allowing only authorized network traffic to pass through according to traffic-filtering rules.

General Information or Data—Information that may include records, documents, or files pertaining to law enforcement operations, such as computer-aided dispatch (CAD) data, incident data, and management information. Information that is maintained in a records management, CAD system, etc., for statistical/retrieval purposes. Information may be either resolved or unresolved. The record is maintained per statute, rule, or policy.

Homeland Security Information—As defined in Section 892(f)(1) of the Homeland Security Act of 2002 and codified at 6 U.S.C. § 482(f)(1), homeland security information means any information possessed by a federal, state, or local agency that (a) relates to a threat of terrorist activity; (b) relates to the ability to prevent, interdict, or disrupt terrorist activity; (c) would improve the identification or investigation of a suspected terrorist or terrorist organization; or (d) would improve the response to a terrorist act.

Identification—A process whereby a real-world entity is recognized and its identity established. Identity is operationalized in the abstract world of information systems as a set of information about an entity that uniquely differentiates it from other similar entities. The set of information may be as small as a single code, specifically designed as an identifier, or a collection of data, such as a given and family name, date of birth, and address. An organization's identification process consists of the acquisition of the relevant identifying information.

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

Information—Includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists. Information received by law enforcement agencies can be categorized into four general areas: general data, including investigative information; tips and leads data; suspicious activity reports; and criminal intelligence information.

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

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

Intelligence-Led Policing (ILP)—A process for enhancing law enforcement agency effectiveness toward reducing crimes, protecting community assets, and preparing for responses. ILP provides law enforcement agencies with an organizational framework to gather and use multisource information and intelligence to make timely and targeted strategic, operational, and tactical decisions.

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

Law—As used by this policy, law includes any local, state, or federal constitution, statute, ordinance, regulation, executive order, policy, or court rule, decision, or order as construed by appropriate local, state, or federal officials or agencies.

Law Enforcement Information- For purposes of the ISE, law enforcement information means any information obtained by or of interest to a law enforcement agency or official that is both (a) related to

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

Lawful Permanent Resident—A foreign national who has been granted the privilege of permanently living and working in the United States.

Least Privilege Administration—A recommended security practice in which every user is provided with only the minimum privileges needed to accomplish the tasks he or she is authorized to perform.

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

Maintenance of Information—Applies to all forms of information storage. This includes electronic systems (for example, databases) and non-electronic storage systems (for example, filing cabinets). To meet access requirements, an organization is not required to create new systems to maintain information or to maintain information beyond a time when it no longer serves an organization's purpose.

Metadata—In its simplest form, metadata is information (data) about information, more specifically information about a particular aspect of the collected information. An item of metadata may describe an individual content item or a collection of content items. Metadata is used to facilitate the understanding, use, and management of information. The metadata required for this will vary based on the type of information and the context of use.

Need to Know— As a result of jurisdictional, organizational, or operational necessities, access to sensitive information or intelligence is necessary for the conduct of an individual's official duties as part of an organization that has a right to know the information in the performance of a law enforcement, homeland security, or counter-terrorism activity, such as to further an investigation or meet another law enforcement requirement.

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

Originating Agency—The agency or organizational entity that documents information or data, including source agencies that document SAR (and when authorized ISE-SAR) information that is collected by a fusion Center.

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

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

Personal Information—Information that can be used, either alone or in combination with other information, to identify individual subjects suspected of engaging in criminal activity, including terrorism. See also Personally Identifiable Information.

Personally Identifiable Information—One or more pieces of information that, when considered together or in the context of how the information is presented or gathered, are sufficient to specify a unique individual. The pieces of information can be:

- Personal characteristics (such as height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation, place of birth, mother's maiden name, distinguishing features, and biometrics information, such as fingerprints, DNA, and retinal scans).
- A unique set of numbers or characters assigned to a specific individual (including name, address, phone number, social security number, e-mail address, driver's license number, financial account or credit card number and associated PIN number, Automated Integrated Fingerprint Identification System [AIFIS] identifier, or booking or detention system number).
- Descriptions of event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records).
- Descriptions of location(s) or place(s) (including geographic information systems [GIS] locations, electronic bracelet monitoring information, etc.).

Persons—Executive Order 12333 defines "United States persons" as United States citizens, aliens known by the intelligence agency concerned to be permanent resident aliens, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. For the intelligence community and for domestic law enforcement agencies, "persons" means United States citizens and lawful permanent residents.

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

Privacy Policy—A printed, published statement that articulates the policy position of an organization on how it handles the personal information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, dissemination, and access. The purpose of the privacy policy is to articulate that the Center will adhere to those legal requirements and Center policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well-

developed and implemented privacy policy uses justice entity resources wisely and effectively; protects the Center, the individual, and the public; and promotes public trust.

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

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

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

For 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.

Public—Public includes:

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

Public does not include:

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

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

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

Redress—Laws, policies, and procedures that address public agency responsibilities with regard to access/disclosure and correction of information and the handling of complaints from persons regarding protected information about them which is under the Center’s control and which is exempt from disclosure and not disclosed to the individual to whom the information pertains.

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

Retention—Refer to Storage.

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

Right to Privacy—The right to be left alone, in the absence of some reasonable public interest in gathering, retaining, and sharing information about a person’s activities. Invasion of the right to privacy can be the basis for a lawsuit for damages against the person or entity violating a person’s privacy.

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

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

Source Agency—Source agency refers to the agency or organizational entity that originates SAR (and when authorized, ISE-SAR) information.

Storage—In a computer, storage is the place where data is held in an electromagnetic or optical form for access by a computer processor. There are two general usages:

1. Storage is frequently used to mean the devices and data connected to the computer through input/output operations—that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-computer storage. This meaning is probably more common in the IT industry than meaning 2.
2. In a more formal usage, storage has been divided into (1) primary storage, which holds data in memory (sometimes called random access memory or RAM) and other “built-in” devices such as the processor’s L1 cache, and (2) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations.

Primary storage is much faster to access than secondary storage because of the proximity of the storage to the processor or because of the nature of the storage devices. On the other hand, secondary storage can hold much more data than primary storage.

With regard to the ISE, storage (or retention) refers to the storage and safeguarding of terrorism-related information, to include homeland security information, terrorism information, and law enforcement information relating to terrorism or the security of our homeland by both the originator of the information and any recipient of the information.

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

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

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

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

Weapons of Mass Destruction (WMD) information was defined and included in the definition of “terrorism information” by P.L. 110-53.

Tips and Leads Information or Data—Generally uncorroborated reports or information generated from inside or outside a law enforcement agency that allege or indicate some form of possible criminal activity. Tips and leads are sometimes referred to as suspicious incident report (SAR), 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 data. Tips and leads information does not include incidents that do not have a criminal offense attached or indicated, criminal history records, or CAD data. Tips and leads information should be maintained in a secure system, similar to data that rises to the level of reasonable suspicion.

A tip or lead can come from a variety of sources, including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information may be based on mere suspicion or on a level of suspicion that is less than “reasonable suspicion” and, without further information or analysis, it is unknown whether the information is accurate or useful. Tips and leads information falls between being of little or no use to law enforcement and being extremely valuable depending on the availability of time and resources to determine its meaning.

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

APPENDIX B: ISE PRIVACY GUIDELINES

Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment

1. Background and Applicability

- a. Background. Section 1016(d) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) calls for the issuance of guidelines to protect privacy and civil liberties in the development and use of the “information sharing environment” (ISE). Section 1 of Executive Order 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans, provides that, “[t]o the maximum extent consistent with applicable law, agencies shall ... give the highest priority to ... the interchange of terrorism information among agencies ... [and shall] protect the freedom, information privacy, and other legal rights of Americans in the conduct of [such] activities” These Guidelines implement the requirements under the IRTPA and EO 13388 to protect information privacy rights and provide other legal protections relating to civil liberties and the legal rights of Americans in the development and use of the ISE.
- b. Applicability. These Guidelines apply to information about United States citizens and lawful permanent residents that are subject to information privacy or other legal protections under the Constitution and Federal laws of the United States (“protected information”). For the intelligence community, protected information includes information about “United States persons” as defined in Executive Order 12333. Protected information may also include other information that the U.S. Government expressly determines by Executive Order, international agreement, or other similar instrument, should be covered by these Guidelines.

2. Compliance with Laws

- a. General. In the development and use of the ISE, all agencies shall, without exception, comply with the Constitution and all applicable laws and Executive Orders relating to protected information.
- b. Rules Assessment. Each agency shall implement an ongoing process for identifying and assessing the laws, Executive Orders, policies, and procedures that apply to the protected information that it will make available or access through the ISE. Each agency shall identify, document, and comply with any legal restrictions applicable to such information. Each agency shall adopt internal policies and procedures requiring it to:
 - (i) only seek or retain protected information that is legally permissible for the agency to seek or retain under the laws, regulations, policies, and executive orders applicable to the agency; and
 - (ii) ensure that the protected information that the agency makes available through the ISE has been lawfully obtained by the agency and may be lawfully made available through the ISE.

- c. Changes. If, as part of its rules assessment process, an agency:
 - (i) identifies an issue that poses a significant risk to information privacy rights or other legal protections, it shall as appropriate develop policies and procedures to provide protections that address that issue;
 - (ii) identifies a restriction on sharing protected information imposed by internal agency policy, that significantly impedes the sharing of terrorism information, homeland security information, or law enforcement information (as defined in Section 13 below) in a manner that does not appear to be required by applicable laws or to protect information privacy rights or provide other legal protections, it shall review the advisability of maintaining such restriction;
 - (iii) identifies a restriction on sharing protected information, other than one imposed by internal agency policy, that significantly impedes the sharing of information in a manner that does not appear to be required to protect information privacy rights or provide other legal protections, it shall review such restriction with the ISE Privacy Guidelines Committee (described in Section 12 below), and if an appropriate internal resolution cannot be developed, bring such restriction to the attention of the Attorney General and the Director of National Intelligence (DNI). The Attorney General and the DNI shall review any such restriction and jointly submit any recommendations for changes to such restriction to the Assistant to the President for Homeland Security and Counterterrorism, the Assistant to the President for National Security Affairs, and the Director of the Office of Management and Budget for further review.

3. Purpose Specification

Protected information should be shared through the ISE only if it is terrorism information, homeland security information, or law enforcement information (as defined in Section 13 below). Each agency shall adopt internal policies and procedures requiring it to ensure that the agency's access to and use of protected information available through the ISE is consistent with the authorized purpose of the ISE.

4. Identification of Protected Information to be Shared through the ISE

- a. Identification and Prior Review. In order to facilitate compliance with these Guidelines, particularly Section 2 (Compliance with Laws) and Section 3 (Purpose Specification), each agency shall identify its data holdings that contain protected information to be shared through the ISE, and shall put in place such mechanisms as may be reasonably feasible to ensure that protected information has been reviewed pursuant to these Guidelines before it is made available to the ISE.
- b. Notice Mechanisms. Consistent with guidance and standards to be issued for the ISE, each agency shall put in place a mechanism for enabling ISE participants to determine the nature of the protected information that the agency is making available to the ISE, so that such

participants can handle the information in accordance with applicable legal requirements. Specifically, such a mechanism will, to the extent reasonably feasible and consistent with the agency's legal authorities and mission requirements, allow for ISE participants to determine whether:

- (i) the information pertains to a United States citizen or lawful permanent resident;
- (ii) the information is subject to specific information privacy or other similar restrictions on access, use or disclosure, and if so, the nature of such restrictions; and
- (iii) there are limitations on the reliability or accuracy of the information.

5. Data Quality

- a. Accuracy. Each agency shall adopt and implement procedures, as appropriate, to facilitate the prevention, identification, and correction of any errors in protected information with the objective of ensuring that such information is accurate and has not erroneously been shared through the ISE.
- b. Notice of Errors. Each agency, consistent with its legal authorities and mission requirements, shall ensure that when it determines that protected information originating from another agency may be erroneous, includes incorrectly merged information, or lacks adequate context such that the rights of the individual may be affected, the potential error or deficiency will be communicated in writing to the other agency's ISE privacy official (the ISE privacy officials are described in section 12 below).
- c. Procedures. Each agency, consistent with its legal authorities and mission requirements, shall adopt and implement policies and procedures with respect to the ISE requiring the agency to:
 - (i) take appropriate steps, when merging protected information about an individual from two or more sources, to ensure that the information is about the same individual;
 - (ii) investigate in a timely manner alleged errors and deficiencies and correct, delete, or refrain from using protected information found to be erroneous or deficient; and
 - (iii) retain protected information only so long as it is relevant and timely for appropriate use by the agency, and update, delete, or refrain from using protected information that is outdated or otherwise irrelevant for such use.

6. Data Security

Each agency shall use appropriate physical, technical, and administrative measures to safeguard protected information shared through the ISE from unauthorized access, disclosure, modification, use, or destruction.

7. Accountability, Enforcement and Audit

- a. Procedures. Each agency shall modify existing policies and procedures or adopt new ones as appropriate, requiring the agency to:
 - (i) have and enforce policies for reporting, investigating, and responding to violations of agency policies relating to protected information, including taking appropriate action when violations are found;
 - (ii) provide training to personnel authorized to share protected information through the ISE regarding the agency's requirements and policies for collection, use, and disclosure of protected information, and, as appropriate, for reporting violations of agency privacy-protection policies;
 - (iii) cooperate with audits and reviews by officials with responsibility for providing oversight with respect to the ISE; and
 - (iv) designate each agency's ISE privacy official to receive reports (or copies thereof if the agency already has a designated recipient of such reports) regarding alleged errors in protected information that originate from that agency.
- b. Audit. Each agency shall implement adequate review and audit mechanisms to enable the agency's ISE privacy official and other authorized officials to verify that the agency and its personnel are complying with these Guidelines in the development and use of the ISE.

8. Redress

To the extent consistent with its legal authorities and mission requirements, each agency shall, with respect to its participation in the development and use of the ISE, put in place internal procedures to address complaints from persons regarding protected information about them that is under the agency's control.

9. Execution, Training, and Technology

- a. Execution. The ISE privacy official shall be responsible for ensuring that protections are implemented as appropriate through efforts such as training, business process changes, and system designs.
- b. Training. Each agency shall develop an ongoing training program in the implementation of these Guidelines, and shall provide such training to agency personnel participating in the development and use of the ISE.
- c. Technology. Where reasonably feasible, and consistent with standards and procedures established for the ISE, each agency shall consider and implement, as appropriate, privacy enhancing technologies including, but not limited to, permissioning systems, hashing, data anonymization, immutable audit logs, and authentication.

10. Awareness

Each agency shall take steps to facilitate appropriate public awareness of its policies and procedures for implementing these Guidelines.

11. Non-Federal Entities

Consistent with any standards and procedures that may be issued to govern participation in the ISE by State, tribal, and local governments and private sector entities, the agencies and the PM-ISE will work with non-Federal entities seeking to access protected information through the ISE to ensure that such non-Federal entities develop and implement appropriate policies and procedures that provide protections that are at least as comprehensive as those contained in these Guidelines.

12. Governance

- a. **ISE Privacy Officials.** Each agency's senior official with overall agency-wide responsibility for information privacy issues (as designated by statute or executive order, or as otherwise identified in response to OMB Memorandum M-05-08 dated February 11, 2005), shall directly oversee the agency's implementation of and compliance with these Guidelines (the "ISE privacy official"). If a different official would be better situated to perform this role, he or she may be so designated by the head of the agency. The ISE privacy official role may be delegated to separate components within an agency, such that there could be multiple ISE privacy officials within one executive department. The ISE privacy official shall be responsible for ensuring that (i) the agency's policies, procedures, and systems are appropriately designed and executed in compliance with these Guidelines, and (ii) changes are made as necessary. The ISE privacy official should be familiar with the agency's activities as they relate to the ISE, possess all necessary security clearances, and be granted the authority and resources, as appropriate, to identify and address privacy and other legal issues arising out of the agency's participation in the ISE. Such authority should be exercised in coordination with the agency's senior ISE official.
- b. **ISE Privacy Guidelines Committee.** All agencies will abide by these Guidelines in their participation in the ISE. The PM shall establish a standing "ISE Privacy Guidelines Committee" to provide ongoing guidance on the implementation of these Guidelines, so that, among other things, agencies follow consistent interpretations of applicable legal requirements, avoid duplication of effort, share best practices, and have a forum for resolving issues on an inter-agency basis. The ISE Privacy Guidelines Committee is not intended to replace legal or policy guidance mechanisms established by law, executive order, or as part of the ISE, and will as appropriate work through or in consultation with such other mechanisms. The ISE Privacy Guidelines Committee shall be chaired by the PM or a senior official designated by the PM, and will consist of the ISE privacy officials of each member of the Information Sharing Council. If an issue cannot be resolved by the ISE Privacy Guidelines Committee, the PM will address the issue through the established ISE governance process. The ISE Privacy Guidelines Committee should request legal or policy guidance on questions relating to the implementation of these Guidelines from those agencies having responsibility or authorities for issuing guidance on such questions; any such requested guidance shall be provided promptly by the appropriate agencies. As the ISE

- governance process evolves, if a different entity is established or identified that could more effectively perform the functions of the ISE Privacy Guidelines Committee, the ISE Privacy Guidelines Committee structure shall be modified by the PM through such consultation and coordination as may be required by the ISE governance process, to ensure the functions and responsibilities of the ISE Privacy Guidelines Committee remain priorities fully integrated into the overall ISE governance process.
- c. Privacy and Civil Liberties Oversight Board. The Privacy and Civil Liberties Oversight Board (PCLOB) should be consulted for ongoing advice regarding the protection of privacy and civil liberties in agencies' development and use of the ISE. To facilitate the performance of the PCLOB's duties, the ISE Privacy Guidelines Committee will serve as a mechanism for the PCLOB to obtain information from agencies and to provide advice and guidance consistent with the PCLOB's statutory responsibilities. Accordingly, the ISE Privacy Guidelines Committee should work in consultation with the PCLOB, whose members may attend Committee meetings, provide advice, and review and comment on guidance as appropriate.
 - d. ISE Privacy Protection Policy. Each agency shall develop and implement a written ISE privacy protection policy that sets forth the mechanisms, policies, and procedures its personnel will follow in implementing these Guidelines. Agencies should consult with the ISE Privacy Guidelines Committee as appropriate in the development and implementation of such policy.

13. General Provisions

a. Definitions

- (i) The term "agency" has the meaning set forth for the term "executive agency" in section 105 of title 5, United States Code, but includes the Postal Rate Commission and the United States Postal Service and excludes the Government Accountability Office.
- (ii) The term "protected information" has the meaning set forth for such term in paragraph 1(b) of these Guidelines.
- (iii) The terms "terrorism information," "homeland security information," and "law enforcement information" are defined as follows:

"Terrorism information," consistent with section 1016(a)(4) of IRTPA means all relating to (A) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism, (B) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations, (C) communications of or by such groups or individuals, or (D) groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

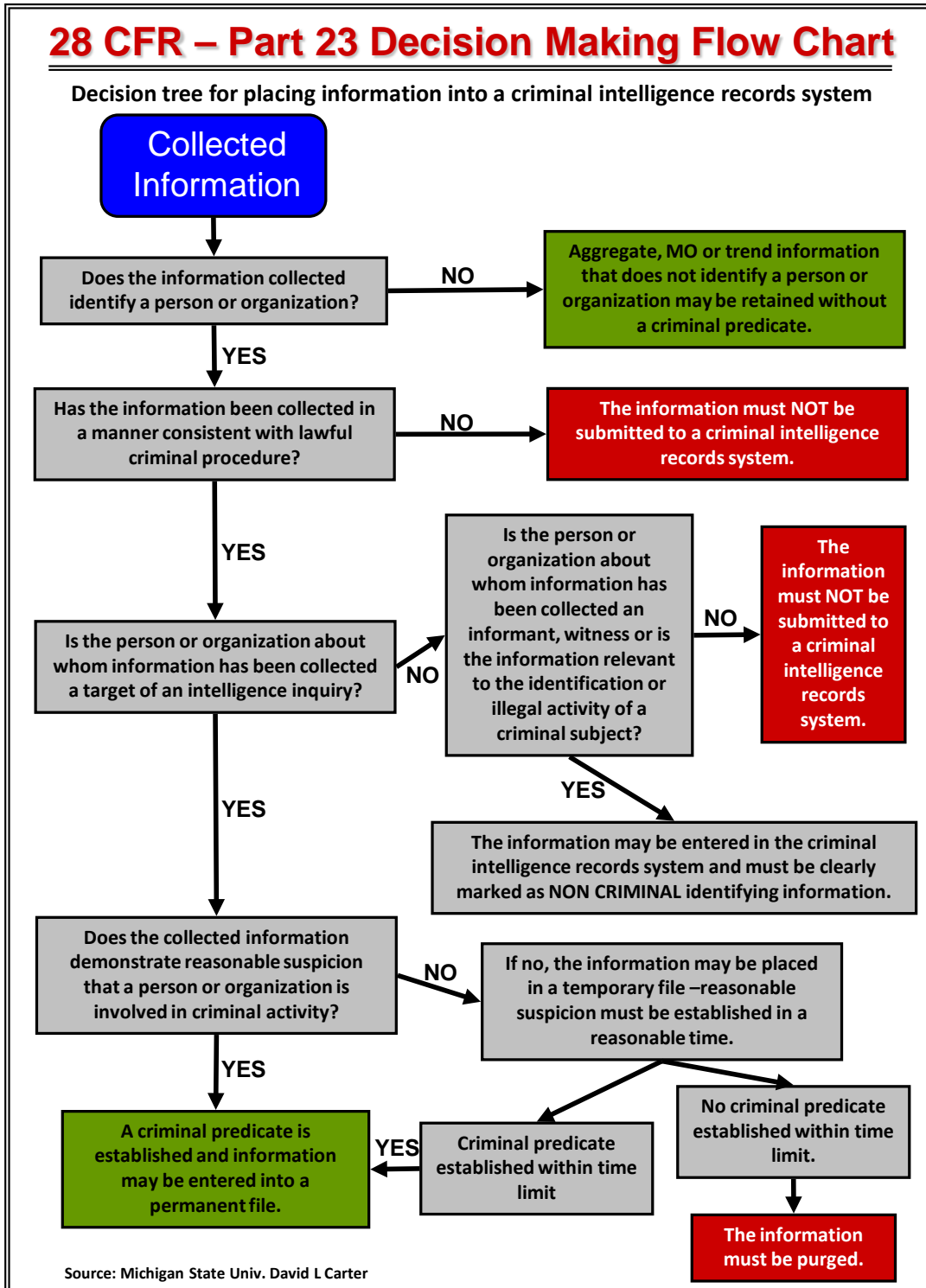
"Homeland security information," as derived from section 482(f)(1) of the Homeland Security Act of 2002, means any information possessed by a Federal,

State, local, or tribal agency that relates to (A) a threat of terrorist activity, (B) the ability to prevent, interdict, or disrupt terrorist activity, (C) the identification or investigation of a suspected terrorist or terrorist organization or any person, group, or entity associated with or assisting a suspected terrorist or terrorist organization, or (D) a planned or actual response to a terrorist act.

“Law enforcement information” for the purposes of the ISE means 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.

- b. The treatment of information as “protected information” under these Guidelines does not by itself establish that the individual or entity to which such information pertains does in fact have information privacy or other legal rights with respect to such information.
- c. Heads of executive departments and agencies shall, to the extent permitted by law and subject to the availability of appropriations, provide the cooperation, assistance, and information necessary for the implementation of these Guidelines.
- d. These Guidelines:
 - (i) shall be implemented in a manner consistent with applicable laws and executive orders, including Federal laws protecting the information privacy rights and other legal rights of Americans, and subject to the availability of appropriations;
 - (ii) shall be implemented in a manner consistent with the statutory authority of the principal officers of executive departments and agencies as heads of their respective departments or agencies;
 - (iii) shall not be construed to impair or otherwise affect the functions of the Director of the Office of Management and Budget relating to budget, administrative, and legislative proposals; and
 - (iv) are intended only to improve the internal management of the Federal Government and are not intended to, and do not, create any rights or benefits, substantive or procedural, enforceable at law or in equity by a party against the United States, its departments, agencies, or entities, its officers, employees, or agencies, or any other person.

APPENDIX C: 28 CFR PART 23 FLOW CHART



APPENDIX D: CIAC STANDARD OPERATING PROCEDURES AND PRODUCT DISSEMINATION

Purpose:

This Colorado Information Analysis Center (CIAC) Standard Operating Procedure (SOP) provides guidance on the procedures, requirements, and liabilities for distribution of CIAC products. This SOP applies to all persons who receive and distribute CIAC products or the information contained in the products.

General:

CIAC documents contain proprietary, legally privileged information. As such, they are legally protected or otherwise exempt from release under the Freedom of Information Act and similar state and local disclosure laws.

Requirements for Receipt of Products:

- a. All recipients of CIAC products are required to have a signed Non-Disclosure Agreement on file with the CIAC.
- b. A person requesting receipt of CIAC products must have a valid need-to-know as determined by the CIAC for Law Enforcement Sensitive or For Official Use Only information.
 - i. Law Enforcement Sensitive: For access to Law Enforcement Sensitive information, an individual must work in an enforcement, investigative or intelligence function or in direct support of an enforcement, investigative or intelligence function. Individuals employed by a non-law enforcement agency (i.e. Colorado Division of Homeland Security and Emergency Management (DHSEM), etc.), must directly support the Homeland Security mission and the individual requires access to meet their official responsibilities.
 - ii. For Official Use Only: For access to For Official Use Only information, an individual must be a verifiable employee of a law enforcement or criminal justice agency, emergency first responder agency, function as a Homeland Security Advisor or Coordinator, security manager or operation security manager at critical and non-critical infrastructure facilities, or

***(U//LES)** Four males were observed taking still photos and video of the Republic Plaza and Denver Agency buildings. The suspects were observed taking 360° photos of the building's exterior cameras as well as taking photos and video while they walked around the block. Upon contact, Republic Plaza security identified two of the four suspects. The suspects claimed they were students with CU Denver's language program.*

***(U//FOUO)** Four males were observed taking still photos and video of a prominent downtown Denver office building. The suspects were observed taking 360° photos of the building's exterior cameras as well as taking photos and video while they walked around the block. Upon contact, building security identified two of the four suspects. The suspects claimed they were students with a local university.*

Figure 1. LES vs FOUO Sample Text

be in a position which has direct implications to the security of the community, state or nation.

- c. CIAC staff will verify with the requestor's agency the requestor's information and will determine the level of access needed.
- d. When a person leaves their position or agency and no longer requires access to CIAC products, they will inform the CIAC of the expected date of departure.

Distribution of Information:

- a. Recipients are authorized to further distribute CIAC products within their organization and are responsible for verifying need to know for the information. Recipients are liable if the information is not appropriately protected as outlined in this document.
- b. Dissemination of CIAC products outside of the recipient's agency requires prior written approval from the CIAC
- c. Electronic Distribution
 - i. CIAC products, "Law Enforcement Sensitive" or "For Official Use Only", will not be sent to non-official e-mail addresses, including commercial e-mail addresses such as Yahoo and Gmail.
 - ii. Each e-mail disseminating CIAC information will contain one of the following caveats:
 - (1) Law Enforcement Sensitive information: The attached report contains information that is LAW ENFORCEMENT SENSITIVE (LES) and should be contained within law enforcement channels only. It contains information that may be exempt from public release under the Freedom of Information Act (FOIA) and Colorado Open Records Act (CORA). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with policy relating to LES information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior written approval of the CIAC.
 - (2) For Official Use Only Information: The attached report contains information that is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (FOIA) and Colorado Open Records Act (CORA). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior written approval of the CIAC.

Securing LES and FOUO Information:

- a. When unattended, LES materials will, at a minimum, be stored in a locked file cabinet, locked desk drawer, a locked overhead storage compartment such as a systems furniture credenza, or similar locked compartment. Materials can also be stored in a room or area that has sufficient physical access control measures to afford adequate protection and prevent unauthorized

access by members of the public, visitors, or other persons without a need-to-know, such as a locked room, or an area where access is controlled by a guard, cipher lock, or card reader.

- b. Laptop computers and other media containing sensitive information will be stored and protected to prevent loss, theft, unauthorized access, and unauthorized disclosure.

Destruction:

- a. "Hard Copy" materials will be destroyed by shredding, burning, pulping or pulverizing, to assure destruction beyond recognition and reconstruction. After destruction, materials may be disposed with normal waste.
- b. Electronic storage media shall be sanitized appropriately by overwriting or degaussing. Contact local IT security personnel for additional guidance.
- c. Paper products containing FOUO or LES information will not be disposed of in regular trash or recycling receptacles unless the materials have first been destroyed as specified above.

Liability:

The unauthorized disclosure of sensitive information by recipients could cause damage or irreparable injury to future or ongoing investigations and operations. The unauthorized disclosure of sensitive information may result in the termination of access to CIAC information, criminal prosecution, and/or the application of a court order prohibiting disclosure of sensitive information.

The protection and security of sensitive information is an important part in the security and safety of our state and our nation's fight against crime and terrorism. If there are any questions regarding information security or dissemination as outlined in this SOP, contact the CIAC at 1-877-509-CIAC (2422) or cdps_ciac@state.co.us

Definitions:

- a. Access – The ability and opportunity to obtain knowledge of classified or sensitive information.
- b. Authorized Person (Recipient) – A person who has a need-to-know for access to classified or sensitive information in the performance of their official duties and who has been granted a personnel security clearance or authorized access at the required level. The responsibility for determining whether a prospective recipient is an authorized person rests with the person who has possession, knowledge, or control of the classified information involved, and not with the prospective recipient.
- c. Automated Information System (AIS) – An assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.
- d. Document – Any physical medium in or on which information is recorded or stored, to include written or printed matter, audiovisual materials, and electromagnetic storage media.

- e. For Official Use Only (FOUO) – information which warrants a degree of protection and administrative control that meets the criteria for exemption from public disclosure under the Privacy Act, and state and federal Freedom of Information Acts.
- f. Information Security – The system of policies, procedures, and requirements established to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security, the state’s security, critical infrastructure/key resource’s security, or the integrity of law enforcement investigations.
- g. Law Enforcement Sensitive (LES) – information that could adversely affect ongoing investigations, create safety hazards for officers, divulge sources of information, and/or compromise their identities.
- h. Need-to-Know – A determination made by an authorized holder of classified or sensitive information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.
- i. Safeguarding – Measures and controls that are prescribed to protect classified or sensitive information.
- j. Sensitive Information – Proprietary, confidential and legally privileged information legally protected or otherwise exempt from release under the Freedom of Information Act and similar State and local disclosure laws.
- k. Unauthorized Disclosure – A communication or physical transfer of classified or sensitive information to an unauthorized recipient.
- l. Violation – Any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified and/or sensitive information.