



Illinois State Police
Statewide Terrorism & Intelligence Center
Privacy Policy
April 2014

Article I. Mission Statement	3
Article II. Compliance and Governance.....	3
Article III. Definitions	4
Article IV. STIC Overview	6
A. Intelligence Personnel	6
B. Division of Administration (DOA) Personnel	7
C. STIC Data Sources	7
Article V. General Operating Procedures.....	8
A. Criminal Intelligence File	8
B. Open Source Search	9
C. Standards for Initiating an Intelligence Query.....	9
D. Standards for Initiating an Open Source Query.....	9
E. Intelligence Collection Standards/Record Entry	10
F. Social Security Numbers	11
G. Data Quality	11
H. Classifications	12
I. Labeling	13
J. Dissemination	13
K. Review and Purge Procedures.....	14
L. Security Procedures	15
M. Training.....	16
Article VI. STIC Data Sources.....	17
A. Law Enforcement Data Sources.....	17
B. Criminal Intelligence Data Stores	20
C. Public Data Sources including Commercial Systems.....	20
D. Flow of Information.....	21
Article VII. – Suspicious Activity Reports (SARs).....	22
A. Standards for Initiating a Query of the Department of Homeland Security (DHS) Information Sharing Environment (ISE) SAR Database.....	23
B. Collection Standards/Record Entry	23
C. Dissemination.....	24
D. Security Procedures	24
E. Applicability	25
Article VIII. Authorized Persons and Users	25
A. Authorized persons	25
B. Authorized users	25
Article IX. Data Quality	26
A. Ownership of data	26
B. Verifying the accuracy of STIC Law Enforcement Data Sources.....	26
C. Verifying the accuracy of STIC Criminal Intelligence Data Stores.....	26
D. Merged Data	27

E. Access and Review	27
F. Record Challenges	27
Article X. Access and Dissemination of Law Enforcement Data Sources	28
A. Access.....	28
B. Dissemination.....	28
Article XI. Accountability	29
A. Programmatic audit logs.....	29
B. Secondary dissemination logs.....	29
C. Monitoring system use and conducting audits.....	29
D. Violations.....	30
E. Penalties.....	30
F. ISP Statewide VITAL Coordinator	30
G. VITAL Quality Control	30

Article I. Mission Statement

The mission of the Illinois State Police (ISP) Statewide Terrorism & Intelligence Center (STIC) is to collect, evaluate, analyze, and disseminate information and intelligence data regarding criminal, terrorist and all-hazards¹ activities.² The STIC is comprised of intelligence and public safety officials from federal, state, and local law enforcement agencies whose primary goal is to provide timely, accurate, and actionable intelligence to public safety and private-sector partners. STIC operations enhance public safety, facilitate communication between agencies, and provide support in the fight against terrorism and criminal activity.

This Privacy Policy applies to all individuals unless otherwise specified. It describes how personally identifiable information is collected, used and secured by STIC. This Policy was prepared by the ISP Privacy Office and is designed to protect the privacy rights of U.S. citizens and other specified individuals.

Article II. Compliance and Governance

All intelligence personnel, participating agency personnel, private contractors, and other authorized individuals³ are required to abide by this Privacy Policy and applicable laws which govern the treatment of the information the center collects, receives, maintains, archives, accesses, or discloses. All intelligence personnel are required to provide written acknowledgement of receipt of this Privacy Policy and written agreement with its compliance. Nothing in this policy is intended to create a private right of action for any member of the public or alter existing or future federal and state law requirements.

¹ "All-hazards" is defined as events or incidents including, but not limited to, major accidents, natural disasters, and terrorist-related activity.

² 20 ILCS 2605/2605-45(4).

³ Hereinafter referred to as "intelligence personnel."

STIC has adopted standard operating procedures and policies that comply with federal and Illinois law⁴ concerning the appropriate collection, analysis, dissemination and retention of personally identifiable information and intelligence data.

The Illinois State Police Director has the primary responsibility for the overall operation of STIC including, but not limited to, its information systems, personnel, and operations.

Reports regarding alleged violations and suggestions for amendments shall be submitted to the Illinois State Police Privacy Office.⁵

Article III. Definitions

- (1) **Actionable intelligence** - a relatively small piece or pieces of non-obvious detail(s) that can form an initial basis point for hypothesis building.
- (2) **Authorized persons** - Terrorism Research Specialists, Criminal Intelligence Analysts, Watch Officers, field intelligence personnel, public safety officials, certified police officers, and other criminal justice administrative and intelligence personnel in the furtherance of their official duties.
- (3) **Authorized users** - Terrorism Research Specialists, Criminal Intelligence Analysts, Watch Officers, field intelligence personnel, public safety officials, certified police officers, and other criminal justice administrative and intelligence personnel who meet certain qualifications outlined in this Policy.
- (4) **Critical Infrastructure Information** – Information not customarily in the public domain and related to the security of critical infrastructure or protected systems - (A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including misuse of or unauthorized access to all types of communications and data transmission systems) that violates federal, state, or local law, harms interstate commerce of the United States, or threatens public health and safety; (B) the ability of critical infrastructure or protected systems to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or, (C) any planned or past operational problem or solution regarding critical infrastructure, including repair, recovery,

⁴ 28 Code of Federal Regulations (CFR) Part 23; 20 ILCS 2605/2605-45(4).

⁵ These reports will be retained subject to the Illinois State Records Act, 5 ILCS 160.

reconstruction, insurance, or continuity to the extent it relates to such interference, compromise, or incapacitation.”⁶

- (5) **Individuals** - encompasses individuals as well as any group, association, corporation, business, partnership or other organization.
- (6) **Personally identifiable information (PII)** - any data that can be used to uniquely identify, contact, or locate a single person or entity.
- (7) **Private right of action** - a term used in United States statutory and constitutional law for circumstances when a court will determine that a law that creates rights also allows private parties to bring a lawsuit, even where no such remedy is expressly provided for in the law.
- (8) **Public safety function** – service whose principal purpose is to protect the safety of life, health, or property. These services may be provided by state or local government entities or may be provided by non-governmental entities including, but not limited to, utility companies and other critical infrastructure industries.
- (9) **Public Safety Official** - a public safety official, serving with or without compensation, working in a public agency in an official capacity, including but not limited to a law enforcement officer, intelligence analyst, firefighter, emergency management official, public health official or member of emergency medical response organization.
- (10) **Private Sector Official** – Vetted official⁷ with health or life safety responsibilities whose agency has signed a Homeland Security and Infrastructure Security Awareness Non-Disclosure Agreement with STIC.
- (11) **Request for Information (RFI)** – a formal request (in person, telephonically, or in writing) to STIC by a public safety or private sector official for information that relates to a public safety function.
- (12) **Suspicious activity** — 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, cyberattacks, testing of security, etc.⁸
- (13) **Suspicious Activity Report (SAR)** — Official documentation of observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity. SAR information offers a standardized means for feeding information repositories or data analysis tools. Patterns identified during SAR information analysis may be investigated in coordination with the reporting agency and, if applicable, a state or regional fusion center. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor is it designed to support interagency calls for service.

⁶ P.L. 107-296, § 212(3).

⁷ A criminal background check is performed on all Private Sector Officials.

⁸ Defined in the Federal Information Sharing Environment-Suspicious Activity Report (ISE-SAR) Functional Standard (Version 1.5).

- (14) **U.S. Citizen** - individuals born in the United States, Puerto Rico, Guam, Northern Mariana Islands, Virgin Islands, American Samoa, or Swain's Island; foreign-born children, under age 18, residing in the U.S. with their birth or adoptive parents, at least one of whom is a U.S. citizen by birth or naturalization; or individuals granted citizenship status by Immigration and Naturalization Services.
- (15) **VITAL** - Violent Crime Information Tracking and Linking system is ISP's data system that stores criminal justice data collected by intelligence personnel.

Article IV. STIC Overview

Section A.	Intelligence personnel
Section B.	Division of Administration Personnel
Section C.	STIC Data Sources

A. Intelligence Personnel

- (1) All STIC and field intelligence personnel (hereinafter referred to as intelligence personnel) are subject to the provisions of this Privacy Policy.
- (2) Intelligence personnel include:
 - (a) **Terrorism Research Specialists** who research and analyze potential terrorism suspect and incident data.
 - (b) **Criminal Intelligence Analysts** who research and analyze potential criminal activity, suspect, and incident data.
 - (c) **Public Safety Officials** – officials who research and analyze incident data and behaviors associated with criminal activity.
 - (d) **STIC Analytical Staff** – Any full-time Illinois State Police Code Employee covered by the Collective Bargaining Agreement between Council 31, American Federation of State, County and Municipal Employees (AFSCME) RC-62 and the State of Illinois, Department of Central management Services who have obtained the job classification Criminal Intelligence Analyst, Terrorism Research Specialist, or Terrorism Research Trainee who provides 24 hour/7 day a week analytical support to the STIC. STIC Analytical Staff members routinely research and analyze data in regard to criminal activity, potential incidents of terrorism, criminal and/or terrorism suspects, and incidents which may be precursors to terrorism related activities, as well as major criminal activity.
 - (e) **STIC Work Group Members** - STIC Analytical Staff and other criminal analyst/program coordinators assigned to the STIC who provide specialized analytical research and data analysis for Violent Crimes, Narcotics, Motor Vehicle Theft, Gaming, Traffic

Safety, the Center for Missing and Exploited Children or any other specialization.

(f) Supervisors

- (i) Watch Officer** – A sworn employee of the Illinois State Police with a rank of Special Agent or Trooper who provides limited supervision, directs the day to day operations of the STIC, provides guidance and assists with the quality control function for STIC Analytical Staff and STIC Work Group Members.
- (ii) Assistant Center Chief (ACC)** – Provides administrative and supervisory oversight to the Watch Officers and Public Safety Officials.
- (iii) Deputy Center Chief (DCC)** – Oversees the functions of STIC and reports to the Center Chief.
- (iv) Center Chief (CC)** – Responsible for all functions and activities of STIC and its employees; provides administrative and supervisory oversight to the ACC.

B. Division of Administration (DOA) Personnel

- (1) Select ISP DOA personnel have access to information contained in law enforcement data systems and criminal intelligence data stores for the limited purpose of providing technical assistance.
- (2) DOA personnel who have access to intelligence data are subject to the provisions of this Privacy Policy.
- (3) Notwithstanding any provisions of this policy to the contrary, DOA personnel shall not disseminate criminal intelligence information.

C. STIC Data Sources

- (1) Intelligence personnel gather information from a variety of data sources. Specifically, personnel access information contained in law enforcement data systems, criminal intelligence data stores, and publicly available records. Depending upon the type of investigation or potential criminal conduct, intelligence personnel query certain specified data sources and compile information about individuals or groups for appropriate dissemination in accordance with this Policy.⁹
 - (a) Law Enforcement Data Systems** – Intelligence personnel may access traditional sources of law enforcement data.

⁹ Given the availability of more modern non-intelligence information sources such as the Internet, newspapers, motor vehicle administration records, CHRI, and other public record information on-line, such sources shall not be considered part of criminal intelligence systems, and shall not be covered by 28 CFR Part 23, even if criminal intelligence systems access such sources during searches on criminal suspects. Therefore, criminal intelligence systems may conduct searches across the spectrum of non-intelligence systems without those systems being brought under 28 CFR Part 23.

- (b) **Criminal Intelligence Data Stores** – Intelligence personnel have access to intelligence information submitted by law enforcement agencies and maintained internally.
- (c) **Publicly Available Records** - Intelligence personnel may access public records through various public and privately compiled sources.

Article V. General Operating Procedures

Section A.	Criminal Intelligence File
Section B.	Open Source Search
Section C.	Standards for Initiating an Intelligence Query
Section D.	Standards for Initiating an Open Source Query
Section E.	Collection Standards/Record Entry
Section F.	Social Security Numbers
Section G.	Data Quality
Section H.	Classifications
Section I.	Labeling
Section J.	Dissemination
Section K.	Review and Purge Procedures
Section L.	Security Procedures
Section M.	Training

The U.S. Department of Justice has promulgated administrative rules at 28 Code of Federal Regulations (CFR) Part 23. These regulations were designed to bring about an equitable balance between the civil rights and liberties of citizens and the needs of law enforcement to collect and disseminate criminal intelligence on the conduct of identifiable persons and groups who may be engaged in systematic criminal activity. The following procedures are intended to implement these regulations and apply to STIC operations and personnel absent a more stringent provision adopted herein.

A. Criminal Intelligence File

- (1) A criminal intelligence file consists of stored information on the activities and associations of:
 - (a) Individuals who are reasonably suspected of being involved in the actual or attempted planning, organizing, financing, or commission of criminal acts; or
 - (b) Individuals who are reasonably suspected of being involved in criminal activities with known or suspected crime figures; or
 - (c) Organizations, businesses, and groups that are reasonably suspected of being substantially and significantly involved in the actual or attempted planning, organizing, financing, or commission of criminal acts (criminal organizations); or
 - (d) Organizations, businesses, and groups that are reasonably suspected of being operated, controlled, financed, or infiltrated

by known or suspected crime figures for use in an illegal manner.

- (2) Types of Crimes Resulting in the Creation of an Intelligence File
 - (a) Any suspected crime that, in the reasonable judgment of the submitting agency or officer, represents a significant and recognized threat to the population and: (1) poses a threat to the life or property of citizens; (2) involves a permanent criminal organization; or (3) is not limited to one jurisdiction.

B. Open Source Search

Information from the worldwide web or Internet that is available to the public. Open source data may or may not require a login identification (ID) or password. Open source information is generally obtained from, but not limited to, search engines, media, public data, social media, blogs, forums, chat rooms, as well as uploaded documents, pictures, and videos. STIC shall retain all open source search information but shall recheck its validity prior to disseminating at a later date.

C. Standards for Initiating an Intelligence Query

Intelligence personnel may perform a criminal intelligence inquiry for law enforcement officials¹⁰ upon request and:

- (1) upon a showing of reasonable suspicion of a crime;¹¹ or
- (2) upon a showing that the query is related to an ongoing criminal investigation; or
- (3) for terrorism screening center encounters. Criminal predicate exists for all individuals listed on Federal and International Watch Lists. These Watch Lists include, but are not limited to the following: Transportation Security Administration (TSA) No Fly List, Terrorism Screening Center (TSC) Watch List, Terrorist Identities Datamart Environment (TIDE), Terrorist Screening Database (TSDB), INTERPOL Red Notices, and the Violent Gang and Terrorist Organization File (VGTOF); or
- (4) for prisoner transports; or
- (5) where necessary to avoid imminent danger to life or property.¹²

D. Standards for Initiating an Open Source Query

- (1) Intelligence personnel may perform an open source query for public safety officials and private sector officials only for a valid public

¹⁰ Intelligence personnel shall disseminate criminal intelligence information only to law enforcement authorities who agree to follow procedures regarding information receipt,

¹¹ The reasonable suspicion requirement represents a higher standard than required by 28 CFR Part 23.20(e); Queries will not be conducted based solely upon violation of traffic laws.

¹² A criminal intelligence inquiry may be performed and the results may be disseminated to a government official or to any other individual, when necessary, to avoid imminent danger to life or property. 28 CFR Part 23.20(f)(1) and (f)(2).

safety purpose. If the official is not a law enforcement officer, the public safety or private sector official may not receive PII unless it is the result of an open source search.

- (2) In order to create STIC products (i.e., threat assessments, intelligence notes) for dissemination to law enforcement, public safety or private sector officials.

E. Intelligence Collection Standards/Record Entry

- (1) Intelligence personnel may collect and maintain criminal intelligence information concerning an individual or a group reasonably suspected of criminal conduct or activity.
- (2) Intelligence personnel will collect and maintain a record of the source of the information.¹³
- (3) For purposes of this Policy, reasonable suspicion is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise.
- (4) Intelligence personnel are responsible for establishing the existence of reasonable suspicion of criminal activity prior to submitting information about an individual or group into any intelligence data system.
- (5) Information submitted to an intelligence system must be relevant to the suspected criminal activity and subject identification.
- (6) Criminal intelligence information that intelligence personnel submit to an intelligence system shall be labeled to indicate the level of sensitivity of the record and the level of confidence in the information in accordance with this Policy.
- (7) STIC systems may include non-criminal identifying information¹⁴ in a criminal intelligence information submission, provided sufficient precautions are in place to make it clear to users the two different types of data that are being accessed.¹⁵
- (8) The ISP retains the right to reject any data element that is not relevant or that could pose an unreasonable risk of harm to the public.
- (9) Investigative techniques employed by Intelligence personnel shall be lawful and only so intrusive as to gather sufficient information to prevent criminal conduct or the planning of criminal conduct.

¹³ The record of the source of the information shall contain, where relevant and appropriate: (1) the name of the originating department, component, and subcomponent; (2) the name of the agency system from which the information is disseminated; (3) the date the information was collected and the date its accuracy was last verified; and (4) the title and contact information for the person to whom questions regarding the information should be directed.

¹⁴ Non-criminal identifying information is information that pertains to an individual, organization, group, or business that is not suspected of criminal involvement but the information is relevant to a criminal suspect

¹⁵ The 1998 Policy Clarification to 28 CFR Part 23.

- (10) Intelligence personnel may not collect and maintain information concerning race, ethnicity, citizenship, place of origin, age, disability, gender, sexual orientation, political, religious, or social views, associations, or activities of any individual or any group unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in such criminal conduct or activity.

F. Social Security Numbers

- (1) Intelligence personnel may not collect, use, or disclose a social security number except:
- (a) to agents, employees, contractors, or subcontractors of a governmental entity or disclosure by a governmental entity to another governmental entity or its agents, employees, contractors, or subcontractors if disclosure is necessary in order for the entity to perform its duties and responsibilities; and, if disclosing to a contractor or subcontractor, prior to such disclosure, the governmental entity must first receive from the contractor or subcontractor a copy of the contractor's or subcontractor's policy that sets forth how the requirements imposed under this Act on a governmental entity to protect an individual's social security number will be achieved;
 - (b) pursuant to a court order, warrant, or subpoena;
 - (c) in order to ensure the safety of: state and local government employees; persons committed to correctional facilities, local jails, and other law enforcement facilities or retention centers; wards of the state; and all persons working in or visiting a state or local government agency facility;
 - (d) for internal verification or administrative purposes.
- (2) Any other collection, use or disclosure of a social security number pursuant to 5 ILCS 179/1 must be approved by the STIC Assistant Center Chief, Deputy Center Chief or Center Chief.

G. Data Quality

- (1) Prior to entering information into any intelligence system, intelligence personnel shall evaluate the reliability of each data source and assess the content validity of the data. Proper labels shall be applied to all data submitted to an intelligence system.
- (2) If intelligence personnel have cause to believe the data contains an error or deficiency, they must contact the VITAL Quality Control Crime Information Evaluator for coordination with the source of the data.
- (3) Random VITAL audits are performed on a continual basis by VITAL Quality Control.
- (4) Intelligence personnel shall use the following labels for source reliability:

- (a) Highly Reliable - The reliability of the source is unquestioned or has been well tested in the past.
 - (b) Usually Reliable - The reliability of the source can usually be relied upon as factual. The majority of information provided in the past has proven to be reliable.
 - (c) Not Often Reliable - The reliability of the source has been sporadic in the past.
 - (d) Unknown -The reliability of the source cannot be judged. Its authenticity or trustworthiness has not yet been determined by either experience or investigation.
- (5) ISP VITAL maintains a record of the source of the information.¹⁶
- (6) Intelligence personnel shall use the following labels for content validity:
- (a) Factual - The information has been corroborated by an investigator or another independent, reliable source.
 - (b) Possibly True - The information is consistent with past accounts.
 - (c) Hearsay - The information is inconsistent with past accounts.
 - (d) Unknown - The authenticity of the information has not yet been determined by either experience or investigation.
- (7) A data element with a source reliability of "Unknown" and a validity assessment of "Unknown" may not be entered into an intelligence system.
- (8) Intelligence personnel will respond to any requests from authorized users for validation of previously disseminated data and, when information is identified that may be inaccurate or incomplete, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the rights of an individual may be affected, provide notice to authorized users who are known to have received the information.¹⁷

H. Classifications

- (1) Prior to entering information into any intelligence system, intelligence personnel shall classify the data in order to protect sources, investigations, and the data subject's right to privacy. Intelligence personnel will treat information pertaining to any individual with the exact same level of privacy protection. Classification also indicates whether internal approval must be completed prior to the release of the information to persons outside STIC.
- (2) STIC classifies data into the following categories:
- (a) **Confidential** – Confidential information is the highest level of unclassified but sensitive information. Access to information defined as "confidential" is limited, even among law enforcement officers.
 - (b) **Law Enforcement Sensitive (LES)** – LES information is middle level unclassified but sensitive information. LES may contain

¹⁶ *Supra* note 13.

¹⁷ As required by 28 CFR Part 23.20(h).

PII and may be disseminated to law enforcement personnel only.

(c) **For Official Use Only (FOUO)** – FOUO is unclassified information of a sensitive nature which can be disseminated outside the scope of law enforcement personnel (i.e., participating agency personnel, private contractors, and other authorized individuals). FOUO will not contain dates of birth or social security numbers. FOUO may contain an individual's photo but only where that photo relates to the individual's record of conviction.¹⁸ FOUO may not be released to the general public.

(d) **Protected Critical Infrastructure Information (PCII)** – Protected Critical Infrastructure Information (PCII) is a subset of Critical Infrastructure Information for which protection is requested under the PCII Program by the requestor. PCII may not be released to the general public.

(e) **Open Source** – Open source information is any information that is publicly available. This information will be marked as "Unclassified" using an indicator of (U). Open Source information may not be released to the general public.

(3) **Classification** - All intelligence information has its security classification marked directly on the information file.

(4) **Re-evaluation of Classification**

Re-evaluations can be based upon time (i.e., tied to the five-year retention/renewal); the addition of new information; or at the time of a request for the information.

I. Labeling

- (1) All criminal intelligence information disseminated will be labeled as such so that the recipient can handle the information in accordance with applicable legal requirements.
- (2) Information labeled as non-criminal identifying information will be maintained and disseminated in the same manner as intelligence information.
- (3) The data contained within STIC criminal intelligence systems will be identified as intelligence or non-criminal identifying information and any applicable legal requirements for handling such data indicated is provided in paragraph E of this Article.

J. Dissemination

- (1) Intelligence personnel may disseminate criminal intelligence information only to law enforcement or criminal investigative authorities who agree to follow procedures regarding the receipt, maintenance,

¹⁸ Training materials used for training purposes may contain an individual's photo that does not relate to the individual's record of conviction.

security, and dissemination of information that are consistent with 28 CFR Part 23 and this Policy.

- (2) Intelligence personnel may disseminate criminal intelligence information to law enforcement or criminal investigative authorities who demonstrate a need and right to know the information in the performance of a law enforcement activity.¹⁹
- (3) Intelligence personnel may disseminate a threat assessment of criminal intelligence information to any individual where necessary to avoid imminent danger to life or property.²⁰
- (4) An access log/audit trail or dissemination record is required when the database is accessed or information is disseminated from the intelligence system. This record can be created automatically by the database, or policies and procedures can be implemented to handle the access log/audit trail or dissemination record manually. The dissemination record shall contain the following information:
 - (a) The date of dissemination of the information;
 - (b) The name of the individual requesting the information;
 - (c) The name of the agency requesting the information;
 - (d) The reason for the release of the information (i.e., a description of the need to know and right to know);
 - (e) The information provided to the requester; and
 - (f) The name of the individual from STIC disseminating the information.
- (5) Secondary dissemination of STIC data is permissible provided the dissemination would have been allowable directly from STIC systems under the terms of this Policy.
- (6) FOUO, PCII and Open Source information contained within the Threat Assessment may be disseminated outside law enforcement only to authorized individuals with a need and a right to know the information.

K. Review and Purge Procedures²¹

- (1) Intelligence personnel will make every reasonable effort to ensure that information maintained in intelligence systems about individuals is current, accurate, and relevant. To accomplish this, intelligence personnel shall annually review intelligence information. The maximum retention period is five years, unless the intelligence information is validated and updated to ensure continuing compliance with system submission criteria.

¹⁹ Need to know is established where the prospective recipient requires access to specific information in order to perform or assist in a lawful and authorized governmental function (i.e., access is required for the performance of official duties). Right to know is established where the prospective recipient is an authorized individual acting in furtherance of a valid law enforcement or public safety function.

²⁰ 28 CFR Part 23.20(f)(2) provides that criminal intelligence information may be disseminated "to a government official or to any other individual, when necessary, to avoid imminent danger to life or property."

²¹ 28 CFR Part 23; 20 ILCS 2605/2605-45(4).

- (2) STIC intelligence databases automatically run daily checks for data that has met the five-year retention period. Data that has not been validated is purged.
- (3) The entire record including all accompanying descriptive, identifying, and non-criminal identifying data must be validated. A record must be maintained of the name of the reviewer, date, and explanation of why the information is retained. Once validated, the retention period for the information may be extended for up to five more years.
- (4) If the information has not been updated and/or validated, it must be removed from the system at the end of the retention period. Material purged from the intelligence system shall be destroyed.²²
- (5) Information removal must be approved by STIC Chief or designee.
- (6) STIC will retain a record of dates when information is to be removed (purged) if not validated prior to the end of its five-year period.
- (7) Non-criminal identifying information will be maintained and/or destroyed in accordance with the Illinois State Records Act.²³

L. Security Procedures

- (1) STIC is committed to protecting privacy and maintaining the integrity and security of personal information. STIC shall be responsible for implementing the following security requirements for its intelligence systems.
- (2) STIC has formally adopted the Criminal Justice Information Systems (CJIS) Security Policy of the U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division²⁴ and applies these provisions to STIC operations. STIC will develop a separate security policy.
- (3) Firewalls are in place to prevent unauthorized agencies or entities from accessing STIC resources.
- (4) **Role-based user access** – The intelligence systems that intelligence personnel access utilize various levels of role-based user access.
 - (a) Each user's role shall determine the types of information accessible to the user.
 - (b) Each user's role contains certain permissions to modify or delete records.
- (5) **Security breaches and security breach notification** – ISP will monitor and respond to security breaches or breach attempts.²⁵
 - (a) In the event that intelligence personnel become aware of a breach of the security of unencrypted personal information, ISP will notify an individual about whom personal information was or is reasonably believed to have been obtained by an

²² Electronic records are permanently deleted and paper files are shredded.

²³ 5 ILCS 160/.

²⁴ May 2006 Version 4.3.

²⁵ See 815 ILCS 530/.

unauthorized person and access to which threatens the physical or financial harm to the person.

- (b) Any necessary notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or any measures necessary to determine the scope of the release of information and if necessary, to reasonably restore the integrity of any information system affected by this release.
- (6) **Physical Safeguards** – STIC systems shall be located in a physically secured area that is restricted to designated authorized personnel.
 - (a) Only designated authorized personnel will have access to information stored in the STIC data systems.
 - (b) All authorized visitors, regardless of agency, are required to register with designated authorized personnel prior to gaining admission to the facility.
 - (c) All authorized registered visitors will be escorted by designated authorized personnel for the duration of the visit.
- (7) **Disaster Recovery** – ISP has appropriate disaster recovery procedures for STIC data outlined in ISP's Disaster Recovery Plan.
- (8) **Information Security Officers** - Federal agencies housed at STIC each have a dedicated information security officer. STIC has an Information Security Officer who is trained and handles network access/security.
- (9) **Assessment Storage** - Risk and vulnerability assessments are stored separately from law enforcement and intelligence data. Risk and vulnerability assessments are not available to the public.

M. Training

(1) Personnel Training

- (a) STIC has adopted the Department of Homeland Security Standards as the education and training standard for its Terrorism Research Specialists, Criminal Intelligence Analysts, and Public Safety Officials.
- (b) All intelligence personnel are provided training on this Privacy Policy.
- (c) DOA personnel who have access to STIC data are provided training on this Privacy Policy.
- (d) Training is provided on this Privacy Policy to all intelligence personnel, including Watch Officers and Management (Center Chief and Assistant Center Chief).
- (e) STIC will provide training to personnel authorized to access and/or disseminate data, including terrorism-related data.
- (f) The ISP Privacy Officer is a licensed attorney and a Certified Information Privacy Professional.

- (g) Private sector personnel in contractual relationships with ISP STIC will receive training on this Privacy Policy.
- (h) All intelligence personnel with access to social security numbers in the course of performing their duties will be trained on ISP's Identity Protection Policy pursuant to the Identity Protection Act.²⁶

(2) Policy Awareness

- (a) This Privacy Policy will be displayed for general view on the ISP website.
- (b) Individuals authorized to access or disseminate intelligence information from STIC will be provided access to and acknowledge a thorough understanding of this Privacy Policy.

(3) Policy Updates

- (a) The ISP Privacy Officer will update this Privacy Policy as new information sources are accessed through STIC.
- (b) The ISP Privacy Officer will monitor legislative activity and update this Privacy Policy accordingly.
- (c) The ISP Privacy Office will review this Privacy Policy annually and update it accordingly.
- (d) Updated policies will contain the policy revision date and version number.
- (e) Individuals authorized to access or disseminate intelligence information from STIC will be informed of policy updates as they become effective.

Article VI. STIC Data Sources

Section A.	Law Enforcement Data Sources
Section B.	Criminal Intelligence Data Stores
Section C.	Public Data Sources
Section D.	Flow of Information

A. Law Enforcement Data Sources

Data from the following systems is not aggregated into a central database or repository. Rather, an analyst accesses each system separately to acquire relevant records related to a data subject. This list is not static but may change in the future as databases are merged, new databases are added or databases that do not prove useful to the mission of STIC are removed.

- (1) The Illinois Law Enforcement Agencies Data System (LEADS) is a statewide, computerized, telecommunications system, maintained by the Illinois State Police, designed to provide the Illinois criminal justice

²⁶ Illinois State Police Directive SRV-200 – Information Security and Disposal of Personal Information.

community with access to computerized justice-related information from both the state and national level. Data within LEADS includes, but is not limited to, active warrants, federal criminal information and files from the Illinois Secretary of State (SOS).

- (2) Citizen and Law Enforcement Analysis and Reporting system (CLEAR) is an information technology system managed by the Chicago Police Department enabling Chicago police to quickly share police incident report data and crime mapping software, among other types of information.
- (3) El Paso Intelligence Center (EPIC) provides timely and expeditious information to federal, state, local, tribal, and international law enforcement agencies concerning drug interdiction and trafficking, alien and weapon smuggling, counterterrorism and other criminal activities. The systems queried include EPIC's in house computer, TECS (U.S. Customs and Treasury), NADDIS (DEA), INS (including border crossings), FAA (Federal Aviation Association) and SENTRY-BOP.
- (4) Mid-State Organized Crime Information Center (MOCIC) is part of the overall Regional Information Sharing Systems (RISS) network. This network searches multiple databases and provides access to criminal intelligence information in the region.
- (5) Illinois Secretary of State (SOS) offers access to its data via LEADS. This access provides digital driver's license photographs & VISAGE Facial Recognition System data.
 - (a) STIC will not store SOS information; Rather STIC will contain a link to LEADS which will, in turn, provide for access to the SOS database.
 - (b) SOS data available through this link includes a subject's name, address, date of birth, gender, and digital image.
- (6) The Offender Tracking System (OTS) database is managed by the Illinois Department of Corrections. OTS provides various forms of information on individuals who have been entered into the Illinois Correctional system.
- (7) Illinois Department of Public Aid database provides access to information on wanted suspects, public aid and medicaid fraud, and sex offenders.
- (8) The Law Enforcement Online (LEO) system is maintained by the FBI and provides a secure network that LEO members – including the law enforcement community, criminal justice officials, first responders, public safety officials, and members of the intelligence and counterintelligence communities – can use to store, process, and transmit sensitive but unclassified information.
- (9) The U.S. Department of Justice Regional Data Exchange System (RDEx) is part of the Department's Law Enforcement Information Sharing Program (LEISP). RDEx includes information to facilitate regional sharing initiatives which serves to further the LEISP's principal

purpose of ensuring that criminal law enforcement information is available for users at all levels of government so that they can more effectively investigate, disrupt, and deter criminal activity, including terrorism, and protect the national security.

- (10) Illinois State Police INDICES - indexed Illinois State Police case records database.
- (11) Targeted Violence Information Sharing System (TAVISS) is a pointer system administered by the U.S. Secret Service National Threat Assessment Center and consists of a database of subjects who have threatened or inappropriately communicated with protectees from federal, state and local agencies.
- (12) Transportation Safety Administration Federal Air Marshal Service Tactical Information Sharing System (TISS) is a database system that stores information, including photos, from suspicious activity reports, incident and arrest reports, and other sources for immediate retrieval and analysis.
- (13) Financial Crimes Enforcement Network (FinCEN) is managed by the U. S. Department of Treasury and provides information to safeguard against financial crime, including terrorist financing, money laundering, and other illicit activity.
- (14) Suspicious Activity Reports – STIC does not have a tips/leads hot-line system for law enforcement or the public. However, law enforcement agencies and private sector security directors may report suspicious activity directly to STIC. If the suspicious activity reported contains personally identifying information, it must meet the Collection Standards outlined in Article V, Section C of this Policy.
- (15) SAFETNet – a database containing information on Illinois Department of Transportation numbers and safety inspections of commercial motor vehicles.
- (16) Traffic Information and Planning System (TIPS) - contains information regarding prior traffic-related contacts with the ISP.
- (17) Firearm Owner's Identification Database/FTIP - database used to check an individual's record of purchasing and eligibility to purchase firearms.
- (18) I-CASE – Repository for ISP Case Investigations.
- (19) Deconfliction – Repository of event-driven criminal investigations.
- (20) Homeland Security Information Network/Homeland Security State and Local Intelligence Community (HSIN/HS SLIC) – a national secure and trusted Web-based portal for information sharing and collaboration among federal, state, local, tribal, territorial, private sector, and international partners engaged in the homeland security mission.
- (21) National Data Exchange (NDEx) – a repository of criminal justice records, available in a secure online environment, managed by the FBI's Criminal Justice Information Services (CJIS) Division.

B. Criminal Intelligence Data Stores

STIC has two stores of criminal intelligence information – VITAL and the STIC Network Drive. Both of these systems shall comply with 28 CFR Part 23.

- (1) VITAL is a data system that stores criminal justice data collected by intelligence personnel. VITAL is intended to enhance cross-jurisdictional information sharing and to facilitate crime prevention, crime fighting, and counter-terrorism efforts taking place throughout Illinois. Specifically, VITAL stores and disseminates intelligence data to assist crime investigators and patrol officers.
 - (a) **Entries into VITAL** – All data from any of STIC's data sources which meets the requirements of 28 CFR Part 23 may be entered into VITAL. Information that does not meet 28 CFR Part 23 collection standards is not entered into VITAL.
 - (b) **Downloads of VITAL** – Regularly scheduled downloads from the VITAL database to the FBI Regional Data Exchange database (R-DEx) warehouse will occur upon written agreement between ISP and the R-DEx Board.
- (2) The STIC Network Drive contains both intelligence and non-criminal identifying information. Intelligence information will only be stored in specific folders to be designated by STIC Management. The folders containing intelligence information will be easily discernible from others in the network drive to ensure proper security and review of files contained therein.

C. Public Data Sources including Commercial Systems

Data from the following systems is not aggregated into a central database or repository. Rather, an analyst accesses each system separately to acquire relevant records related to a data subject. The ISP may contract with commercial providers to obtain this relevant data. The providers agree in writing to comply with all federal and state laws and provide quality data to industry standards. The ISP will only gather data with agency authority under state law.²⁷ Information will not be collected when the source agency used prohibited means to gather it.

- (1) Lexis-Nexis/Accurint provides background information to government agencies on individuals, businesses, addresses, vehicles, judgments and liens, social security numbers, media news articles, among other data.
- (2) Dun and Bradstreet database provides business information and is also a credit rating provider.
- (3) Westlaw provides access to statutes, case law materials, public records and other legal resources, as well as current news articles and business information.
- (4) National and State Sex Offender Registration Web Sites

²⁷ 20 ILCS 2605/2605-45(4).

- (a) Intelligence personnel will have access to links to public Sex Offender Registration Web Sites.
 - (b) Sex offender registration information available through these links includes a registrant's name, address, physical description, and digital image along with their compliancy status, crime and the county of conviction.
- (5) Federal Bureau of Prisons and State Departments of Corrections (DOC)²⁸ public websites provide inmate information on currently-incarcerated individuals.
 - (a) Intelligence personnel will have access to a link to public DOC websites.
 - (b) DOC information available through these links includes parent institution, inmate status, location, physical description and digital image along with sentencing information and admission, release or discharge data.
- (6) Experian offers online credit reports and credit bureau data.
- (7) Interpol is the largest International Police Association which facilitates cross-border police co-operation, and supports and assists all organizations, authorities and services to prevent or combat international crime.
- (8) National Insurance Crime Bureau (NICB) assists law enforcement in their detection and deterrence of insurance fraud and vehicle theft.
- (9) Methamphetamine Registries
- (10) TLO online Investigation Serve - Commercial Public Records Database.
- (11) Internet – Capability of researching full Internet sources including commercial, educational and governmental networks.

D. Flow of Information

(1) Work-ups

- (a) **Tactical Work-up** - This is a request for information when the requesting law enforcement officer is on an active traffic or criminal stop. The analyst conducts an abbreviated search of intelligence databases with a goal to return the relevant information to the officer within a reasonable time. Once the basic information is relayed to the officer, the analyst completes a full database work-up.
 - (i) LEADS, RDEx, and VITAL will be checked during every tactical work-up. The analysts will check other relevant data sources at their discretion.
- (b) **Full Database Work-up** – The analyst determines the nature of the request, searches all relevant databases and sources of information, documents all information, and disseminates the information as appropriate.

²⁸ For purposes of this Policy, "DOC" refers to the Federal Bureau of Prisons and all state Departments of Correction.

(2) Products

- (a) **Daily Intelligence Notes** – The analyst gathers topic information, researches and verifies that information, receives authorization from the Watch Officer, and disseminates it based upon classification.
- (b) **Intelligence Alerts** – Intelligence alerts (also known as Officer Safety Alerts) can be STIC analyst originated or pass-through products obtained by STIC from other intelligence fusion centers or sources. Intelligence Alerts are not disseminated to the general public.
- (c) **Threat Assessments (TA)** – STIC will compile background and threat information for purposes of providing assessments of special events or critical infrastructure. Examples include, but are not limited to, events with large attendance expected, venues or sites of previous threats, violence or criminal activity, and those events which may have national significance. The ISP Privacy Officer or his/her designee with review and approve all TAs prior to dissemination. FOUO, PCII and Open Source information contained within the TA may be disseminated outside law enforcement within the restrictions of this Privacy Policy. STIC will not complete intelligence work-ups on individuals unless reasonable suspicion exists that the subject in question is involved in criminal activity and that suspected criminal activity has a bearing on the event involved.
- (d) **Be On the Lookout (BOLO)** – BOLOs will be disseminated at the request of officers in the field. A suspect's personally identifiable information will be included in a BOLO when reasonable suspicion exists that the subject in question is involved in criminal activity. A missing person's personally identifiable information will be included in a BOLO when that person is missing under unexplained, involuntary or suspicious circumstances. BOLOs are not entered into LEADS and are only disseminated to law enforcement officers.

Article VII. – Suspicious Activity Reports (SARs)

Section A.	Standards for Initiating a Query
Section B.	Collection Standards/Record Entry
Section C.	Dissemination
Section D.	Security Procedures
Section E.	Applicability

Intelligence personnel are required to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of Suspicious Activity Report information. The search, collection and dissemination restrictions to SAR information outlined in this Article are only applicable

to that information which contains PII as defined in Article III(6) of this Policy. A SAR is an official documentation of observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity.

A. Standards for Initiating a Query of the Department of Homeland Security (DHS) Information Sharing Environment (ISE) SAR Database

- (1) Intelligence personnel may perform a SAR inquiry for law enforcement officials upon request and upon a showing of reasonable suspicion of a crime.
- (2) Intelligence personnel may perform a SAR inquiry, upon request, where necessary to avoid imminent danger to life or property.
- (3) Prior to allowing access to the SAR information, intelligence personnel shall: (1) ensure that attempts to validate or refute the information have taken place; (2) ensure 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 (3) categorize the information as unsubstantiated or uncorroborated if attempts to validate or determine the reliability of the information have been unsuccessful.
- (4) Intelligence personnel will only search SAR information which meets the reasonable suspicion standard and is marked as such.
- (5) Intelligence personnel will use a standard reporting format and data collection codes for SAR information.

B. Collection Standards/Record Entry

- (1) Intelligence personnel are responsible for documenting SAR information into the VITAL database.
- (2) Intelligence personnel shall store only SAR information that meets 28 CFR Part 23 collection standards and is marked as such and which includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other types of information.
- (3) For purposes of this Policy, reasonable suspicion is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise.
- (4) Intelligence personnel may retain SAR information for a period up to five years and shall assign a "disposition" label (for example, undetermined or unresolved, cleared or unfounded, verified, or under active investigation). This disposition label must be attached to the SAR information within one year after it is entered into the database so

that a subsequently authorized user knows the status and purpose for the retention. STIC will retain the information based on the retention period associated with the disposition label.

- (5) If the disposition label is "cleared or unfounded," that SAR information which contains PII will be immediately purged from the DHS ISE SAR database or, at a minimum, the PII will be removed from the SAR file.
- (6) STIC's SAR process provides for human review and vetting to ensure that information is both legally gathered and, where applicable, determined to have a potential terrorism nexus.
- (7) Law enforcement officers and appropriate STIC and participating agency staff will be trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism.

C. Dissemination

Intelligence personnel shall:

- (1) Disseminate only SAR information that rises to the level of reasonable suspicion.
- (2) Disseminate SAR information in response to an interagency inquiry for law enforcement, homeland security, or public safety and analytical purposes or provide an assessment of the information to any agency, entity, individual, or the public when credible information indicates an imminent danger to life or property.
- (3) Disseminate SAR information to law enforcement or criminal investigative authorities who demonstrate a need and right to know the information in the performance of a law enforcement activity.²⁹
- (4) Allow for secondary dissemination of SAR information provided the dissemination would have been allowable directly from STIC systems under the terms of this Policy.

D. Security Procedures

- (1) STIC will adhere to and follow STIC's physical, administrative, and technical security measures to ensure the protection and security of SAR information. SAR information will be secured in a system that is the same as or similar to the system that secures criminal intelligence.
- (2) STIC will secure 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.
- (3) STIC 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

²⁹ *Supra* note 15.

existing policies and protocols utilized to protect the information, as well as information privacy, civil rights, and civil liberties.

- (4) STIC'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.
- (5) STIC 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.

E. Applicability

The general provisions of this Policy apply unless otherwise provided for in this Article.

Article VIII. Authorized Persons and Users

Section A. Authorized persons
Section B. Authorized users

A. Authorized persons

- (1) For purposes of this Policy, authorized persons are Terrorism Research Specialists, Criminal Intelligence Analysts, Watch Officers, field intelligence personnel, public safety officials, certified police officers, and other criminal justice administrative personnel in the furtherance of their official duties.
- (2) Authorized users may disseminate STIC data to authorized persons as defined in this Section only in accordance with the dissemination rules of this Policy.

B. Authorized users

- (1) For purposes of this Policy, authorized users are Terrorism Research Specialists, Criminal Intelligence Analysts, Watch Officers, field intelligence personnel, public safety officials, certified police officers, and other criminal justice administrative personnel, who:
 - (a) Are approved for STIC access by the ISP; and
 - (b) Meet, at a minimum, the certification requirements for STIC access; and

- (c) Undergo training regarding the system's capabilities as well as the appropriate use and sharing of data accessed through STIC.

Article IX. Data Quality

Section A.	Ownership of data
Section B.	Verifying the accuracy of STIC Law Enforcement Data Sources
Section C.	Verifying the accuracy of STIC Intelligence Stores
Section D.	Merged Data
Section E.	Access and Review
Section F.	Record Challenges

A. Ownership of data

- (1) All data accessed through a law enforcement or public data source is considered to be the property of that source.
- (2) Because it retains ownership of the data, each source is ultimately responsible for the quality and accuracy of its data.
- (3) STIC notifies the originating agency or the originating agency's privacy officer when the center reviews the quality of the information it has received from an originating agency and identifies data that: (1) may be inaccurate or incomplete; (2) may include incorrectly merged information; (3) may be out of date; (4) cannot be verified; or (5) lacks adequate context such that the rights of the individual may be affected.
- (4) Notification pursuant to Section (A)(3) above is documented via e-mail to STIC Supervisors, consistent with Article IV (A)(2)(d), who ensure the information is not entered into VITAL.
- (5) All data entered into VITAL and the STIC Network Drive is deemed the property of the Illinois State Police.
- (6) Any connections to the VITAL database must allow for intelligence personnel to edit, alter or remove information pursuant to this Policy.

B. Verifying the accuracy of STIC Law Enforcement Data Sources

Inaccurate information can have a damaging impact upon the data subject and the integrity and functional value of STIC query responses. Any information obtained through a query to STIC from law enforcement data sources must be independently verified with the original source from which the data was extrapolated before any official action (e.g., search warrant application or arrest) is taken. Law enforcement officers and agencies are responsible for verifying the quality and accuracy of the data.

C. Verifying the accuracy of STIC Criminal Intelligence Data Stores

Any information obtained through a query to STIC from Criminal Intelligence Data Stores must be independently verified with the original source from which the data was extrapolated before any official action (e.g., search warrant application or arrest) is taken. Law enforcement officers and agencies are responsible for verifying the quality and accuracy of the data.

D. Merged Data

- (1) Due to the potential harm caused by inaccurate merging of information, data about an individual from two or more sources will not be merged by a STIC Terrorism Research Specialist or Criminal Intelligence Analyst unless the identifiers or characteristics, when combined, clearly establish that the information from multiple records is about the same individual or organization.
- (2) If the matching requirements cannot fully be met but there is an identified partial match, the information may be merged only if accompanied by a statement that it has not been adequately established that the information relates to the same individual or organization.

E. Access and Review

- (1) In order to avoid interference with criminal investigations, members of the public cannot access STIC or individually identifiable information on themselves or others.³⁰
- (2) Persons wishing to access data pertaining to themselves should communicate directly with the source of the data in question.³¹
- (3) Reports regarding alleged violations and suggestions for amendments shall be submitted to the Illinois State Police Privacy Office.³²

F. Record Challenges

Persons wishing to challenge records should communicate directly with the agency source of the data in question.

³⁰ Requests for this information are treated as Illinois Freedom of Information Act requests and will be retained consistent with that statute. See 5 ILCS 140.

³¹ STIC will not provide these individuals with a list of sources.

³² If an individual has a complaint or objection to the accuracy or completeness of terrorism-related information that has been or may be shared through the ISE that: (a) is held by the STIC; (b) allegedly resulted in harm to the complainant; and (c) is exempt from public disclosure, the STIC will inform the individual of the procedure for submitting, if needed, and resolving complaints or objections. Complaints will be received by Lt. Kathleen deGrasse, ISP Privacy Officer, at the following address: 9511 W. Harrison St., Des Plaines, IL 60016. The STIC will acknowledge the complaint and state that it will be reviewed, but will not confirm the existence of the information that is exempt from disclosure. If the information did not originate with the STIC, STIC will notify the originating agency in writing and, upon request, assist such agency to correct or purge any identified data/record deficiencies or to verify that the record is accurate. Any personal information originating with the STIC will be reviewed and corrected in or deleted from STIC data/records if it is determined to be erroneous, include incorrectly merged information, or be out of date. The ISP Privacy Office will maintain records of complaints and correction requests and the resulting action, if any.

Article X. Access and Dissemination of Law Enforcement Data Sources

Section A. Access
Section B. Dissemination

A. Access

- (1) Access permissions, generally
 - (a) The information accessed through STIC is information that has been accessible to law enforcement officers for many years. STIC technology will permit authorized users to retrieve and analyze these same records in an efficient and timely manner as a law enforcement investigative tool.
 - (b) The public shall not have access to STIC data.
- (2) Use for legitimate investigative purposes
 - (a) Information obtained from or through STIC can only be used for official law enforcement investigative purposes.
 - (b) An official law enforcement investigative purpose means that the request for data is directly linked to a law enforcement agency's active criminal case investigation or is in response to a confirmed lead that requires additional corroboration.

B. Dissemination

- (1) Prohibitions on dissemination, generally
 - (a) Except as otherwise provided in this Policy, information obtained from or through STIC:
 - (i) Cannot be sold, published, exchanged, or otherwise disclosed, to the public or for commercial purposes; and
 - (ii) Can only be disseminated to authorized persons.
- (2) Confidentiality
 - (a) Intelligence personnel shall protect the confidentiality of all data entered or accessed through STIC.
- (3) Research purposes
 - (a) The Illinois State Police may use the information accessed through STIC for research purposes in the aggregate, but such aggregate or analyzed data may not be identifiable to any person without the express consent of the individual.
- (4) Secondary dissemination, generally
 - (a) Authorized users may only disseminate information accessed through STIC to other authorized persons in order to fulfill their criminal justice functions.
 - (b) All secondary disseminations must be logged in accordance with Article X of this Policy.

Article XI. Accountability

Section A.	Programmatic audit logs
Section B.	Secondary dissemination logs
Section C.	Monitoring system use and conducting audits
Section D.	Violations
Section E.	Penalties
Section F.	Statewide VITAL Coordinator
Section G.	VITAL Quality Control Unit

Intelligence personnel and agencies accessing STIC data must follow all applicable state and federal laws and regulations, including rules and regulations of the Illinois State Police, regarding the use and dissemination of STIC data.

A. Programmatic audit logs

- (1) Queries to VITAL will be logged by the system and identify the user initiating the query. The dissemination log must contain:
 - (a) A description of the information queried (including the identity or identities to whom the information relates);
 - (b) The date the information was queried;
 - (c) The individual who conducted the query (including their agency and contact information);
 - (d) The authorized person to whom the information was disseminated.

B. Secondary dissemination logs

- (1) When information accessed through STIC is disseminated outside the agency from which the original request is made, a secondary dissemination log must be maintained by the disseminating agency. The dissemination log must contain:
 - (a) A description of the information disseminated (including the identity or identities to whom the information relates);
 - (b) The date the information was released;
 - (c) The individual to whom the information was released (including their agency and contact information); and
 - (d) The purpose for which the information will subsequently be used.
- (2) Whenever information labeled "confidential" is disseminated outside the agency from which the original request was made, the secondary dissemination log must specify the demonstrable need to know.

C. Monitoring system use and conducting audits

- (1) The Illinois State Police is responsible for monitoring the use of all STIC data sources to guard against inappropriate or unauthorized use.

- (2) The Illinois State Police will investigate misuse of STIC data and conduct or coordinate audits concerning the proper use and security of STIC data by users.
- (3) All STIC inquiries by authorized persons will be made available, upon request, to that authorized person's agency.

D. Violations

- (1) When the Illinois State Police learn of a violation of policies, laws, or regulations concerning the use of STIC data, it must notify the chief executive of the offending agency in writing. Agencies must take action to correct such violations and provide an assurance in writing to the STIC Center Chief that corrective action has been taken.
- (2) Any suspected or documented misuse of STIC information discovered by or reported to a law enforcement agency must be reported by that agency to the Illinois State Police.

E. Penalties

- (1) The failure of a law enforcement agency to remedy violations may result in suspension or termination of access to STIC data.

F. ISP Statewide VITAL Coordinator

- (1) The ISP will appoint a Statewide VITAL Coordinator who is responsible for training intelligence personnel in the use of VITAL and 28 CFR Part 23.
- (2) The ISP Statewide VITAL Coordinator will maintain all authorized VITAL users' access forms and certification training materials at the STIC facility.

G. VITAL Quality Control

- (1) The VITAL Quality Control Unit was formulated to ensure and maintain the integrity of the VITAL project database in compliance with 28 CFR Part 23.
- (2) This unit has full and complete authoritative review of all information entered into the VITAL intelligence database.
- (3) A second level of review shall be performed by VITAL Quality Control staff responsible for reviewing all entries of new VITAL users.
- (4) All entries of new users are reviewed for the first 90 days; thereafter, Quality Control staff will randomly review 25 percent of all users' entries.
- (5) Where information is found to be erroneous or deficient such that an individual's privacy rights are impacted, the VITAL Quality Control Crime Information Evaluator's responsibilities are limited to notifying the original source agency in writing for their follow-up and correction.³³

³³ When data is obtained from that source agency, it once again goes through reliability checks prior to labeling. See Article V, Section E of this Policy.



National Security State Information Center's Privacy Policy

STRENGTH THROUGH COLLABORATION

I. Acknowledgements

The National Security State Information Center (NSSIC) Privacy Policy is a living document developed through the joint efforts of the Puerto Rico Office for Public Security Affairs, now known as the Puerto Rico Homeland Security Office (PRHSO), the Puerto Rico Department of Justice and agencies such as the Puerto Rico Emergency Management Agency.

Key members and Agencies which supported this project were:

Rafael Muñoz, PRHSO's Director
Lawyer Karla M. Rivera, Puerto Rico Dept. of Justice
Mr. Orlando Morales PRHSO's
Christina Abernathy and John Wilson, Institute for Intergovernmental Research

In addition, documents such as the Privacy, Civil Rights, and Civil Liberties Policy Templates for Justice Information Systems, and the Freedom of Information Act played a crucial role in the development of this Policy.

II. Introduction

September 11, 2001 will always remain in our memories and in our history as the day we were awakened to the knowledge that Global Terrorism had reached our coasts. It brought into focus the need to reassess our methods of gathering/sharing/using information on terrorists, criminal activities, and the individuals and organizations likely involved. It also highlighted the need to do so in an efficient and effective manner, one that would systematically minimize any negative effect not only on the State but also on the People, and ultimately, The Nation. One aspect crucial in improving our capacity to prevent harm is the use new technology to supply clear, concise, and rapid information to those who will be able to maximize its usage. However, the benefits reaped from this aspect cannot compromise another aspect: ***the individuals' privacy, civil rights, and civil liberties.***

The following privacy policy protects these rights while improving public safety. When individuals are sufficiently comfortable with the integrity of information system operations, they are more likely to cooperate with and support them, thus enhancing public safety and our way of life.

The policy here drawn represents a commitment of the Puerto Rico Fusion Center to uphold the rights granted by U.S. Constitution, the Puerto Rico State laws and other laws adopted over time for the protection of Human Rights and Civil Liberties.

III. Table of Revisions

The following table defines dates and descriptions of changes done to the NSSIC's Privacy Policy through the years, location of changes and the authors of said changes. The table defines the reason for the changes, if the changes are based on corrections, inclusions, omissions, or general changes defined by stakeholders such as State and federal agencies, presidential directives and/or changes in state laws affecting in any way the procedures of the NSSIC. The changes will appear in green Arial 14 font to be easily recognized. The new versions will absorb previous changes to minimize misunderstandings.

Version	Change date	Authors	Description
1	N/A	O. Morales	Original release
2	N/A	O. Morales	Changes include integration into the document of comments from IIR and State laws that can have impact on the privacy policy (stricter, prohibitive, etc.). This revision protocol was not determined until September 7, 2010, so changes were in different fonts/colors.
3	Sept. 7, 2010	K. Rivera, O. Morales	A new format was implemented to streamline the information; the official name of NSSIC was introduced; ISE and SAR information was integrated in the Policy.
4	November 3, 2010		Updated version based on a Webinar session with members of the DOJ/DHS Fusion Center Privacy Technical Assistance providers (Privacy Policy Review Team) to assist NSSIC in complying with the ISE Privacy Guidelines requirements and the DHS/DOJ <i>Fusion Center Privacy Policy Development Template</i> (April 2010).
5	November 9, 2010	K. Rivera, O. Morales	Addition of POC's e-mail addresses and law citations related to information access
6	June 2014	S. Lebrón	POC e-mail updated. Corrected the name of the center: The National Security State Information Center.

Contents

I.	Acknowledgements	2
II.	Introduction	2
III.	Table of Revisions	3
IV.	Policy Provisions	5
A.	Purpose	5
B.	Collection Limitation	6
C.	Data Quality	7
D.	Use Limitation	7
E.	Security Safeguards	8
F.	Openness	9
G.	Individual Participation	9
H.	Accountability	10
V.	Governance	11
VI.	Information Procedures, Processes and Guidelines	13
A.	Information Collection	13
B.	Information Quality Assurance	17
C.	Collation, Analysis and Merging	18
D.	Sharing and Disclosure	19
E.	Redress	23
1.	Disclosure	23
2.	Complaints and Corrections	24
F.	Security Safeguards	25
G.	Information Retention and Destruction	26
H.	Information System Transparency, Accountability and Enforcement	26
I.	Training	28
	Appendix A – Terms and Definitions	30
	Appendix B - Federal Laws Relevant to Seeking, Retaining, and Disseminating Justice Information	40
	Appendix C - State Laws Relevant to Seeking, Retaining, and Disseminating Justice Information	42

IV. Policy Provisions

This *Privacy Policy* embraces the eight Privacy Design Principles developed by the Organization of Economic Cooperation and Development's *Fair Information Practices* while following appropriate privacy and civil liberties safeguards as outlined in the principles and shall be used to guide the policy wherever applicable. The eight Privacy Design Principles are:

- A. **Purpose Specification** — Define agency purposes for information to help ensure agency uses of information are appropriate.
- B. **Collection Limitation** — Limit the collection of personal information to that required for the purposes intended.
- C. **Data Quality** — Ensure data accuracy.
- D. **Use Limitation** — Ensure appropriate limits on agency use of personal information.
- E. **Security Safeguards** — Maintain effective security over personal information.
- F. **Openness** — Promote a general policy of openness about agency practices and policies regarding personal information.
- G. **Individual Participation** — Allow individuals with reasonable access and opportunity to correct errors in their personal information held by the agency.
- H. **Accountability** — Identify, train, and hold agency personnel accountable for adhering to agency information quality and privacy policies.

All these principles have, as common end results, an increase in local public safety and national security, thus minimizing the threat and risk of injury to first responder personnel, the public in general, and all property involved. This task, always taking into consideration the individual privacy, civil rights, civil liberties, and other protected interests will support the integrity of the criminal investigation and the justice system we believe in.

We at the NSSIC will strive to promote our capabilities thus minimizing reluctance of individuals or groups to use or cooperate with the system by creating an atmosphere of governmental legitimacy and accountability which will make the most effective use of our public resources allocated to the public's safety.

A. Purpose

The Puerto Rico State Information Center or Centro de Información del Estado as defined in Spanish is a Fusion Center (herein referenced to as "Center") as defined below:

A Fusion Center is a collaborative effort of two or more agencies who provide resources, expertise, and/or information to the Center with the goal of maximizing the ability to detect, prevent, apprehend, and respond to criminal and terrorism activity. It will also be able to maintain critical communication before, during and after any natural disasters affecting Puerto Rico and the rest of the Nation.

The Center project began to take shape in response to the increased need for timely information sharing and exchange of crime-related information among members of the law enforcement community. One component of the Center focuses on the development and exchange of criminal intelligence. This component focuses on the intelligence process where information is collected, integrated, evaluated, analyzed and disseminated. Another key component of the Fusion Center will also address communications between all agencies that, directly or indirectly, are related to any man-made or natural disasters, thus making the Center an All-Threats/All-Hazards Fusion Center.

The Center's intelligence products and services will be available to law enforcement agencies, other criminal justice entities, and all agencies, and private sector operations based on their need-to-know classification. All agencies participating in the Center will be subject to a Memorandum of Understanding and will be required to adhere to all Center policies and security requirements. The purpose of this privacy policy is to ensure safeguards and sanctions are in place to protect personal information while information analysis and intelligence are developed and exchanged.

The Center will develop databases by using existing data sources from participating entities to integrate data with the goal of identifying, developing, and analyzing information and intelligence related to terrorist activity, and other crimes for investigative leads as well as trends and patterns related to All-Hazards. Examples of such information will be that related to any terrorist activities that might have any tie-ins or include words such as Puerto Rico, local gangs or terrorist groups. Crimes that could be related to organizations within Puerto Rico will also be monitored for evidence of large scale or interstate crime that could or could not be related to terrorist cells. Cyber terrorism or identity theft focused on Puerto Rican citizens living in the mainland will be monitored for origins that could be in Puerto Rico or international origins. All-Hazards will include information relating to spills, fires, accidents or events at Critical Infrastructures or National Monuments, etc. This capability will facilitate integration and exchange of information between the participating agencies.

B. Collection Limitation

The Center is founded and maintained to analyze information and intelligence by agencies participating in the project. The decision of the agencies to participate in the Center and about which databases to provide is voluntary and will be governed by the laws and rules governing the individual agencies respecting such data, as well as by applicable federal and state laws.

Because the laws, rules, or policies governing information and intelligence that can be collected and released on private individuals varies from agency to agency, limitations on the collection of data concerning individuals is the responsibility of the collector of the original source data. Each contributor of information is to abide by the collection limitations applicable to it by reason of law, the Center's and their own policies and

procedures. This will include the proper labeling of information aligned with the Center and all other participating Agencies. Information contributed/generated by the Center will be aligned throughout the program and will be collected in conformance with agreed upon policies and procedures.

C. Data Quality

The agencies participating in the Center remain the owners of the data contributed and are, therefore, responsible for the quality and accuracy of the data accessed by the Center. Inaccurate personal information can have a damaging impact on the person concerned and on the integrity and functional value of the Center. In order to maintain the integrity of the Center, any information obtained through the Center must be independently verified with the original source from which the data was extrapolated *before* any official action (e.g., warrant or arrest) is taken. User agencies and individual users are responsible for compliance with respect to use and further dissemination of such information and the purging and updating of the data.

D. Use Limitation

Information obtained from or through the Center is exclusively for lawful purposes. A lawful purpose means the request for data is directly linked to a law enforcement agency's active criminal investigation or is a response to a confirmed lead that requires follow-up to prevent a criminal act. This includes any terrorist acts or threats within our island or Nationwide and which might have a connection to Puerto Rico in any way.

The **Commander-of-Center (CoC)** will take necessary measures to make certain that access to the Center's information and intelligence resources is secure and will prevent any unauthorized access or use. The Board reserves the right to restrict the qualifications and number of personnel who will be accessing the Center and to suspend or withhold service to any individual violating this *Privacy Policy*. The **Center's Executive Committee (CEC)**, or persons acting on behalf of the CEC, further reserves the right to conduct inspections concerning the proper use and security of the information received from the Center.

Security for information derived from the Center will be provided in accordance with applicable laws, rules, and regulations. Furthermore, all personnel who receive, handle, or have access to Center data and/or sensitive information will be trained as to those requirements. All personnel having access to the Center's data agree to abide by the following rules:

1. The Center's data will be used only to perform official investigative-related duties related to All-Threats/All Hazards in a manner authorized by the user's employer.

2. Individual passwords will not be disclosed to any other person except as authorized by agency management.
3. If authorized personnel of any of the participating agencies or members of the Center suspect their passwords were disclosed or compromised, said passwords will be changed.
4. Background checks will be completed on personnel who will have direct access to the Center.
5. Use of the Center's data in an unauthorized or illegal manner will subject the user to denial of further use of the Center, discipline by the user's employing agency, and/or criminal prosecution.

All NSSIC personnel, participating agency personnel, personnel providing information technology services to the agency, private contractors, 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 (including Information Sharing Environment [ISE] participating centers and agencies), and participating justice and public safety agencies, as well as to private contractors, private entities, and the general public.

All NSSIC 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 list of applicable state and federal privacy, civil rights, and civil liberties laws referenced in Appendices B and C of this policy.

The NSSIC has adopted internal operating policies that are in compliance with applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to the listing of applicable state and federal privacy, civil rights, and civil liberties laws referenced in Appendices B and C of this policy.

Each authorized user understands that access to the Center can be denied or rescinded for failure to comply with the applicable restrictions and use limitations.

E. Security Safeguards

1. Information obtained from or through the Center will not be used or publicly disclosed for purposes other than those specified in the Memorandum of Understanding that each participating agency must sign.
2. Information cannot be (1) sold, published, exchanged, or disclosed for commercial purposes, (2) disclosed or published without prior approval of the contributing agency, or (3) disseminated to unauthorized persons.
3. Use of the Center's data is limited to those individuals who have been selected, approved, and trained accordingly. Access to information contained within the

Center will be granted only to law enforcement and all participating agencies' personnel who have been screened with a state and national fingerprint-based background check, as well as any additional background screening processes using procedures and standards established by the Fusion Center Governance Board.

4. Each individual user will be provided with an electronic copy of this privacy policy and must complete and sign a hard copy of an Individual User Agreement Form after having read the policy acknowledging receipt of the policy and confirming agreement to comply with the policy and provisions here contained. This form will be supplied upon arrival to the Fusion Center and kept in records for 5 years or while the individual maintains connections with the Fusion Center. New Privacy Policy updates will be distributed and Letters of Assignment will be supplied to the Individuals for their signatures. These documents will be kept with the User Agreement Forms initially signed by each Individual. The individual's key information will be stored in a database for future reference as well as to tie-in with the log files. In addition, to confirm each Individual's skills, the Center will be doing a skills review test before granting access. The Center will ask the individual to make a formal request and will deny him access if the skills are not up to requirements defined in the CONOPS.
5. Access to the Center's databases from outside of the Center will only be allowed over secure network lines and with the approval of the Fusion Center Governance Board. A logging system will be implemented to maintain records of the information sought and collected, by whom and when it was collected. This will allow full traceability of queries and their purposes.

F. Openness

The Center will allow access to the Privacy Policy to all personnel working at the Center's database and analysis desks as well as participating agencies that require the support of the Center. The access will be direct for all users that have an actualized user name and password. Only the CoC will have authorization to edit the Policy and only after a review and approval of the NSSIC Privacy Oversight Committee. All participating agencies either will have a representative at the Center or a connection through a secure line, allowing the review of the policy at any time. In addition, the Privacy Policy will be available on the NSSIC's website for the public's review and comments in both English and Spanish.

G. Individual Participation

The data maintained by the Center is provided, on a voluntary basis, by the participating agencies or is information obtained from other sources by the Center. Each individual user searching against the data as described herein will be required to acknowledge that he or she remains solely responsible for the interpretation, further dissemination,

and use of any information that results from the search process. The individual will also be responsible for ensuring that any information relied upon is accurate, current, valid, and complete, especially before any official action is taken in full or partial reliance upon the information obtained.

Members of the public cannot access individually identifiable information, on themselves or others, from the Center's applications. Persons wishing to access data pertaining to themselves will make a formal request to the Center but the data will not identify the originating agency. The Center will communicate directly with the agency or entity that is the source of the data in question and will supply them with the new data supplied by the member of the public requesting the review. If the information is correct, the originating agency will correct their data, will inform the Center, who will inform the inquirer about the correction done.

Participating agencies agree that they will only attend requests related to their agencies.

H. Accountability

Any query request made to the Center's data applications is automatically logged by the system identifying the user initiating the query. When such information is disseminated outside of the agency from which the original request is made, a secondary dissemination log must be maintained in order to correct possible erroneous information and for audit purposes, as required by applicable law. Secondary dissemination of information can only be to a law enforcement agency for a law enforcement investigative purpose or to other agencies as provided by law. The agency *from* which the information is requested will maintain a record (log) of any secondary dissemination of information. This record will reflect as a minimum:

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

The Governance Board will be responsible for conducting or coordinating audits and investigating misuse of the Center's data or information. The Center's CoC or Privacy Officer (when assigned) shall report all violations and/or exceptions to the Board and will serve as the liaison for the Information Sharing Environment. Individual users of the Center's information remain responsible for their legal and appropriate use of the information contained therein. Failure to abide by the restrictions and use limitations for the use of the Center's data may result in the suspension or termination of use privileges, discipline sanctions imposed by the user's employing agency, or criminal prosecution. Each user and participating agency in the Center is required to abide by this *Privacy Policy* in the use of information obtained by and through the Center.

V. Governance

1. Primary responsibility for the operation of the Center, its information systems, operations, personnel coordination; the receiving, and the enforcement of this policy is assigned to the Commander-of-Center (CoC). This will include all operations such as: seeking, retention, evaluation, information quality, analysis, destruction, sharing, or disclosure of information.
2. The Center is guided by three separate but crucial Committees: 1) The Center's Executive Committee, who is the decision-making group as well as manages budgets and key-decisions affecting the Center, and acts as ambassadors of the program, 2) the Center Privacy Oversight Committee, that monitors the Center's Privacy Policy, its proper application and any infringements of this policy and its related Federal and state laws, and 3) the NSSIC Committee, composed of representatives from all the stakeholders involved one way or another, in the NSSIC. This last Committee is basically composed of the suppliers as well as customers of the NSSIC.
 - a. The NSSIC's Executive Committee (EC) is comprised, but not restricted to nine members. These will represent the State's Public Safety agencies as well as the Governor's representatives in matters related to Homeland Security. They have direct authority and ownership in the decision-making and goal setting processes of the Center. The Committee is comprised of the following:
 - ❖ Homeland Security Advisor for Puerto Rico
 - ❖ Superintendent of the Puerto Rico Police Department
 - ❖ Director Puerto Rico Homeland Security Office
 - ❖ Director Puerto Rico Emergency Management Agency
 - ❖ Director Emergency Medical Service
 - ❖ Director Puerto Rico National Guard
 - ❖ Secretary Puerto Rico Department of Justice
 - ❖ Director, Puerto Rico Fire Department
 - ❖ Director HIDTA (honorary)
 - ❖ Any other member appointed by the Governor
 - b. The NSSIC Privacy Oversight Committee (NSSIC-POC) shall be comprised, but not restricted to five members. These members have knowledge of State and/or federal laws relating to privacy policies and would be composed of at least the following:
 - ❖ A trained Privacy Officer (PO) from the Center or the CoC if no PO has been assigned.
 - ❖ A legal counsel representative (Attorney at Law or DOJ)

- ❖ A Law Enforcement Official (Local Law Enforcement or FBI Official)
 - ❖ A representative of the Governor, House of Representatives or the Senate
 - ❖ A representative of Civil, Human Rights Advocates
3. An appointed and trained Center PO (or COC until a PO is appointed) will receive all reports regarding alleged errors and violations of the provisions of the Privacy Policy, receive and coordinate complaint resolution under the center's redress policy, guide the CPOC, act as the liaison between the Information Sharing Environment, the NSSIC-POC, the stakeholders and the Community to ensure the Center adheres to the Provisions for the ISE privacy guidelines as well as all Guidelines defined herewith. The Privacy Officer can be contacted at the following e-mail address: nssic@polcia.gov

In addition, the Privacy Oversight committee liaises with community privacy advocacy groups to ensure that privacy and civil rights are protected within the provisions of this policy and within the center's information collection, retention, and dissemination processes and procedures.

The NSSIC Committee composed of representatives or Fusion Liaison Officers (FLO's) from all the stakeholders involved in the NSSIC bring forth concerns, needs and/or requests from their agencies or groups. In addition, they can submit changes in policies, procedures, and protocols that should be addressed by the NSSIC. All this information is consolidated and brought to the attention of the NSSIC -EC by the CoC during their routine meetings. The Committee is comprised of FLO's from State and Federal Agencies involved in Law enforcement, Public Safety or support both of first responders and Critical Infrastructure. It will, at a later date, include representatives from the Sector Specific Security Groups of Critical Infrastructure within the Territory as well as a representative of the Region Fusion Centers as they become available.

4. When the operation becomes too complex to be handled only by the Commander of Center (increased facility size, data volume handled or personnel attached), a Center Security Officer (CSO) will be hired. The CSO will be responsible for security policy-making, development of security awareness among the staff and stakeholders, risk assessment of information assets, conduct periodic vulnerability assessment and recommend controls in light of the value vs. threat vs. vulnerability vs. cost. Furthermore, he will analyze all logs to initiate preventive measures such as modification of access privileges, deletion of user id's, and review of access privileges on a need-to-know basis.

VI. Information Procedures, Processes and Guidelines

A. Information Collection

1. The Center will seek or retain information that:
 - Is based upon a criminal predicate or threat to public safety, or
 - Is based upon reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or is planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and the information is relevant to the criminal (including terrorist) conduct or activity, or
 - Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime; or
 - Is useful in a crime analysis or in the administration of criminal justice and public safety (including topical searches); or
 - Is based on a level of suspicion that is less than reasonable suspicion, such as tips and leads or suspicious activity reports (SARs) and ISE-SARs; 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, when appropriate.
2. The Center will not seek or retain information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular non-criminal organization or lawful event; or their race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation.
3. Labels will be applied by participating agencies and to center-originated information to indicate to the accessing authorized user that:
 - The information pertains to protected information, to include "personal data" on any individual (as defined in Appendix A of this policy), and, to the extent expressly provided in this policy, includes organizational entities.
 - The information is subject to laws, in Appendices B and C, restricting access, use, or disclosure.
4. The Center personnel will, upon receipt of information, assess the information to determine its nature and purpose and will assign categories to the information (or ensure that the originating agency has assigned categories to the information). Personnel will assign information to categories to indicate the result of the assessment, such as:
 - Whether the information is general data, tips and leads data, suspicious activity reports(SAR's or ISE-SAR's), or criminal intelligence information;

- The nature of the source (for example, anonymous tip, interview, public records, private sector);
 - The reliability of the source (for example, reliable, usually reliable, unreliable, unknown); and
 - The validity of the content (for example, confirmed, probable, doubtful, cannot be judged).
5. At the time a decision is made by the NSSIC to retain information, it will be labeled (by record, data set, or system of records), to the maximum extent feasible, pursuant to applicable limitations on access and sensitivity of disclosure to:
- Protect confidential sources and police undercover techniques and methods.
 - Not interfere with or compromise pending criminal investigations.
 - Protect an individual's right of privacy or their civil rights and civil liberties.
 - Provide legally required protections based on the individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, participant in a witness protection program, or resident of a domestic abuse shelter.
6. The labels assigned to existing information within this section 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.
7. NSSIC 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 suspicious activity report (SAR) information. Center personnel will:
- Prior to allowing access to or dissemination of the information, ensure that attempts to validate or refute the information have taken place and 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 (or a more restrictive) access or dissemination standard that is used for data that rises to the level of reasonable suspicion (for example, "need-to-know" and "right-to-know" access or dissemination for personally identifiable information).

- Regularly provide access to or disseminate the information in response to an interagency inquiry for law enforcement, homeland security, or public safety and analytical purposes or provide an assessment of the information to any agency, entity, individual, or the public when credible information indicates potential imminent danger to life or property.
 - Retain information for three years in order to work an unvalidated tip, lead, or SAR information to determine its credibility and value or assign a "disposition" label (for example, undetermined or unresolved, cleared or unfounded, verified, or under active investigation) so that a subsequently authorized user knows the status and purpose for the retention and will retain the information based on the retention period associated with the disposition label.
 - Adhere to and follow the center's physical, administrative, and technical security measures to ensure the protection and security of tips, leads, and SAR information. Tips, leads, and SAR information will be secured in a system that is the same as or similar to the system that secures data that rises to the level of reasonable suspicion.
8. The NSSIC 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.
9. The labels will also define accessibility and sensitivity of disclosure of said information based on the state and Federal laws regarded in this Policy. All analysts, their supervisors and the Commander of Center will have access to all information gathered in the Center. Liaisons at the participating agencies will have access to information requested, conditioned to the type of information and how it relates to either them or their agencies. The Center's Concept of Operations Manual (NSSIC -CONOPS) defines these same labels and their proper use policy, as well as all other policies and procedures related to the Center. All personnel will be required to adhere to the practices, such as collection, use, analysis, retention, destruction, sharing, and disclosure of information, defined by the CONOPS procedures. These procedures are defined to abide strictly by all state and Federal laws that protect privacy, civil rights, and civil liberties herewith in defined. The primary laws being the U.S. Constitution (First, Fourth, and Sixth Amendments), the Constitution of the Commonwealth of Puerto Rico (Sections 1-20), and the Federal Civil Rights laws, 42 U.S.C. § 1983, United States Code, Title 42, Chapter 21, Subchapter I, § 1983. All other laws and regulations applied to this center, its participants and the information herewith collected are outlined in the Appendixes B and C.
10. The PRISC will identify and review protected information originating from the center prior to sharing that information in the ISE. Further, the Center will provide notice mechanisms, including, but not limited to, metadata or data fields that will enable ISE authorized users to determine the nature of the protected information. This will allow them to handle effectively the information in accordance with applicable legal

requirements. Prior to the implementation of this Privacy Policy, the CONOPS will be released, defining all policies, including SAR Submittal Form and information handling policy, with exact methodology and procedures. They will be defined by type of participating agency and dissemination procedures. One key dissemination policy will be that no information related to on-going or past criminal investigations will be disseminated to non-law enforcement agencies unless specified in writing by the Center's Commander of Center. This is aligned with the 28 CFR Part 23.

11. The NSSIC requires certain basic descriptive information (metadata tags or labels) to be entered and electronically associated with data (or content) for which there are special laws, rules, or policies regarding access, use, and disclosure, including terrorism-related information shared through the ISE. The types of information include:
 - The name of the originating center, department or agency, component, and subcomponent.
 - The name of the center's justice information system from which the information is disseminated.
 - The date the information was collected and, where feasible, the date its accuracy was last verified.
 - The title and contact information for the person to who questions regarding the information should be directed.
12. The NSSIC will attach (or ensure that the originating agency has attached) 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.
13. The NSSIC will keep an electronic record of the source of all information sought and collected by the center.
14. All information gathered through any method of investigative techniques used by the Center and affiliated agencies and handled in any way (collection, use, analysis, retention, destruction, sharing, and disclosure of information) will strictly comply and adhere to the following regulations and guidelines:
 - 28 CFR Part 23
 - Organisation for Economic Co-operation and Development's (OECD) *Fair Information Practices* (except under conditions defined by the Federal Privacy Act; state, local, or agency policy).
 - To criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) *National Criminal Intelligence Sharing Plan* (NCISP).
 - ISE-SAR Functional Standard (Version 1.5)
 - Local, state and federal laws as defined in Appendix B & C.
15. The NSSIC's SAR process provides for human review and vetting to ensure that information is both legally gathered and, where applicable, determined to have a potential terrorism nexus. Law enforcement officers and appropriate center and

participating agency staff will be trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism.

16. The NSSIC's SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals and/or organizations 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.
17. The Center will contract only with commercial database entities that provide an assurance that they gather personally identifiable information in compliance with local, state, and federal laws and which is not based on misleading information collection practices.
18. The Center will not directly or indirectly receive, seek, accept, or retain information from any individual or nongovernmental information provider who may or may not receive a fee or benefit for providing the information, except as expressly authorized by law or center policy; or if the center knows or has reason to believe that the individual or information provider is legally prohibited from obtaining or disclosing the information.
19. If, at any time, the Center develops information gathering and investigative functions, the techniques used will be the least intrusive necessary in the particular circumstance to gather legally authorized information. These procedures will be defined in the NSSIC CONOPS prior to the Center's implementation.
20. External agencies that access the NSSIC'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.

B. Information Quality Assurance

1. The Center will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources of information; accurate; current; complete. It will also include 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 [Refer to Section C: Collation and Analysis] has been met. One method is the labeling of said information based on its level of quality (accurate, complete, current, verifiable, and reliable).
2. The Center will investigate, during its analysis and if part of the program, its investigative phase, in a timely manner, alleged errors and deficiencies and will

correct, delete, or refrain from using protected information found to be erroneous or deficient. The Center will make every reasonable effort to ensure that information will be corrected, deleted from the system, or not used when the Center learns that the information is erroneous, misleading, obsolete, or otherwise unreliable. All methodologies used are defined in the Center's Concept of Operations Manual (NSSIC -CONOPS).

3. The labeling of retained information will be reevaluated when new information is gathered that has an impact on the center's confidence (validity and reliability) in retained information or when 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.
4. The Center will conduct periodic data quality reviews of information it originates and make every reasonable effort to ensure that information will be corrected at the source agency, deleted from the system, or not used when the Center learns that the information is erroneous, misleading, obsolete, or otherwise unreliable.
5. SLT agencies, including agencies participating in the ISE, are responsible for the quality and accuracy of the data accessed by or shared with the Center. Originating agencies providing data remain the owners of the data contributed. The Center will advise the appropriate data owner, in writing, if its data is found to be inaccurate, incomplete, out of date, or unverifiable. This also includes incorrectly merged information, or information that lacks adequate context such that the rights of the individual may be affected.
6. The Center will use written or documented electronic notification to inform recipient agencies when information previously provided by the Center is deleted or changed by the center (for example, it is determined to be inaccurate or includes incorrectly merged information).

C. Collation, Analysis and Merging

1. Information acquired by the Center or accessed (Collation) from other sources will only be analyzed by qualified individuals who have successfully completed a background check and appropriate security clearance, if applicable, and have been selected, approved, and trained accordingly as per procedures outlined in the NSSIC -CONOPS.
2. The information these analysts will evaluate is information as defined in Section VI, A. Information Collection of this policy.
3. This information will be related to any information which might shed light unto a possible criminal or terrorist act to occur or which might have occurred. This includes ties to any known criminal or terrorist organizations, events in which they were/are involved and which might be related to criminal or terrorist acts, etc.

4. Information acquired by the Center or accessed from other sources is analyzed (**Analysis**) according to priorities and needs and will only be analyzed to:
 - Further crime prevention (including terrorism), enforcement, force deployment, or prosecution objectives and priorities established by the Center
 - Provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal (including terrorist) activities.
 - Grant support to agencies during an All-Hazard situation while analyzing any information which could be connected to a terrorist act, group or individual
5. Records about an individual or organization from two or more sources will not be merged (**Merging**) during a routine analysis unless there is sufficient identifying information to reasonably conclude that the information is about the same individual or organization. The set of identifiers sufficient to allow merging will consist of all available attributes that can contribute to higher accuracy of match. The set of identifying information can be, but is not limited to:
 - name (full; partial if there is more evidence supporting the merge)
 - date of birth
 - law enforcement or corrections system identification number
 - Individual identifiers, such as fingerprints, photographs, clearly defined tattoos, or scars; social security number; driver's license number; or other biometrics.
6. If the matching requirements are not fully met but there is an identified partial match, the information may be associated if accompanied by a clear statement that it has not been adequately established that the information relates to the same individual or organization.

D. Sharing and Disclosure

1. The Center will assign clearly defined, credentialed, access to certain individuals as defined in the NSSIC -CONOPS. Each user category or classification will have access to specific types of information. Within the Center, only the CoC, the analysts and their supervisors, will have full access to all information lines available to the Center. They will be the personnel who looks for tendencies, detect threats, or supports criminal investigations for the PRPD, Fire or other law enforcement agencies not only in Puerto Rico but within the Nation's Public Safety Community. This includes other State and Regional Fusion Centers, FBI, and DHS personnel on a need-to-know basis. Other categories of personnel, such as IT, the PIO, or any support staff, do not require access to said information and will be defined so in the NSSIC -CONOPS. The Commander of Center, the PIO and the analyst supervisors will be the only personnel assigned to Information sharing. **No individual within the Center will be capable of editing collected data from participating agencies.** If the Center detects external information requiring editing, the supplying agency will be informed as they have the exclusively right to change it. The Center

will then receive the updated information and share it with any other agency that might be using said information. This will maintain accuracy throughout the system.

2. The NSSIC adheres to the current version of the ISE-SAR Functional Standard for its suspicious activity reporting (SAR) process, including the use of a standard reporting format and commonly accepted data collection codes and a sharing process that complies with the ISE-SAR Functional Standard for suspicious activity potentially related to terrorism.
3. Use of the Center's data is limited to those individuals who have been selected, approved, and trained accordingly. This means that any Fusion Liaison Officer wishing to have access to the Center and its databases will need to follow the same requirements of the Centers analysts. Access to information contained within the Center will be granted only to the Fusion Liaison Officers of law enforcement and participating agencies' personnel which will have been screened with a state and national fingerprint-based background check, as well as any additional background screening processes using procedures and standards established by the Fusion Center Governance Board. They will also receive training in Privacy Policy, Civil Liberties and Rights in accord with the DHS Privacy Office guidelines.
4. The Center personnel who will have access to all information collected, analyzed and merged will be the Intelligence Analysts, their Supervisors, the CSO, and the Commander of Center. The Public Information Officer (PIO) will not have access to this information as well nor will have full privileges. The PIO will be oriented by the CoC or the CSO on what information can be made public.
5. Access to or disclosure of records retained by the Center will be provided to persons within the Center or in other governmental agencies who are authorized to have access and only for legitimate law enforcement, public protection, public prosecution, public health, or justice purposes and only for the performance of official duties in accordance with law and procedures applicable to the agency for whom the person is working. An audit trail will be kept of access by or dissemination of information to such persons as defined in the NSSIC -CONOPS. Participating agencies may not disseminate information received from the Center without approval from the originator of the information, be it the Center itself or any other originating agency as agreed upon signing the Center's MOU.
6. Records retained by the NSSIC may be accessed by or disseminated to those responsible for public protection, public safety, or public health only for public protection, public safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures. An audit trail sufficient to allow the identification of each individual who accessed or received information retained by the center and the nature of the information accessed will be kept by the center.
7. Information gathered or collected and records retained by the NSSIC may be accessed or disseminated for specific purposes upon request by persons authorized

by law to have such access and only for those uses and purposes specified in the law. An audit trail sufficient to allow the identification of each individual who requested, accessed, or received information retained by the center, the nature of the information requested, accessed, or received, and the specific purpose will be kept for a minimum of three years by the center.

8. Information gathered and records retained by the Center may be accessed or disclosed to **a member of the public** only if the information is defined by law to be a public record or otherwise appropriate for release to further the agency mission and is not excepted from disclosure by law. Such information may only be disclosed in accordance with the law and procedures applicable to the Center for this type of information or when there is a legitimate need. An audit trail will be kept of all requests and of what information is disclosed to a member of the public.
9. Information gathered and records retained by the Center **will not** be:
 - Sold, published, exchanged, or disclosed for commercial purposes
 - Disclosed or published without prior notice to the contributing agency that such information is subject to re-disclosure or publication
 - Disseminated to unauthorized persons.
10. There are several categories of records that will ordinarily **not be provided** to the public:
 - Some public records are required to be kept confidential by Federal or Puerto Rico law as they have been deemed exempted from disclosure. Records exempt from disclosure under the Puerto Rico Public Information Law, include:
 - Investigatory records of law enforcement agencies are exempted from disclosure requirements due to the nature of the information and their possible use in criminal investigations. However, certain law enforcement records must be made available for inspection and copying **as long as there availability status does not interfere with a criminal or terrorist related investigation.**
 - Intelligence information, including information subject to 28 CFR Part 23.
 - Protected federal, state, or local records, which may include records owned or controlled by another agency.
 - A violation of the nondisclosure agreement.
 - Puerto Rico court decisions that address exemptions under the Puerto Rico Public Information Law include the following: Colón Cabrera vs. Caribbean Petroleum Corp., 2007 TSPR 48/170 DPR 582 (Hernández Denton); Santiago vs. Bobb, 117 DPR 153,159, and Angueira Navarro vs. Junta de Libertad 2000 TSPR 2, 150 DPR 10 (Negrón García)
 - 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 the Critical Infrastructure Information Act of 2002. This includes a record assembled,

prepared, or maintained to prevent, mitigate, or respond to an act of terrorism or an act of agricultural terrorism, vulnerability assessments, risk planning documents, needs assessments, and threat assessments.

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

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

The above exceptions can be better defined through the following citations from the case of Colón vs. Caribbean Petroleum, 170 DPR 582, (2007). In which it is stated that:

We consider, first of all, if the information which is the object of the request, can be catalogued as public information. It is necessary to do this preliminary determination due to the fact that, once a document is catalogued as public, any citizen has the right to request access to it subject to determined exceptions.

Article 1(b) of the Law of Public Documents, 3 L.P.R.A. 1001(b), defines a public document as "any document which originates, or is kept or received in any dependency of the Commonwealth of Puerto Rico according to the law or in relation to the management of public affairs and that pursuant to the provisions of § 1002 of this title is required to be permanently or temporarily preserved

In our System of law we do not have a special legislation that disposes the exceptions in which the Government of Puerto Rico can maintain certain documents out of the public scrutiny. However, this Court has affirmed the supposed occasions in which the Government can claim confidentiality validly, as: (1) when a law declares so; (2) when the communication is protected by any of the evidentiary privileges that citizens can invoke; (3) when revealing the information can damage fundamental rights of third parties; (4) when it involves the identity of a confidant, and (5) when it is official information according to the Rules 414 and 415 of Evidence. (citations omitted) To maintain the confidentiality, the Government has the responsibility to prove that it satisfies any of the exceptions before mentioned.

In synthesis, all law that pretends to hide information to a citizen under the cloak of confidentiality has to justify itself to plenitude. This is satisfied if the legislation (1) falls within the constitutional power of the government; (2) promotes an important or substantial governmental interest;

Page 593

(3) the governmental interest is not related with the suppression of freedom of expression; and (4) the concomitant restriction of the right to freedom of expression is not larger than the essential to promote said interest. (citations omitted) Thereby, the State can invoke the mantle of secretiveness in cases of imperative public interest. Id

E. Redress

1. Disclosure

1. An individual is entitled to know the existence of and to review the information about him or her, up to a certain degree, which has been gathered and retained by the Center and only upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity. The disclosure of said information is subject to the conditions specified below. The individual may obtain a copy of the information to challenge the accuracy or completeness of the information. 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. All requests and what information is disclosed will be kept on file.
2. The existence, content, and source of the information will not be made available to an individual under Federal or Puerto Rico Public Information Law as defined in section VI.D (Sharing and Disclosure) when:
 - 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 system
 - The information relates to issues related to investigations addressing any criminal or terrorist related incident.
 - The information source does not reside with the Center
 - The Center did not originate or does not own or have a right to disclose the information.

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

3. Types of information which ordinarily will not be disclosed to members of the public upon their request for review are ownership of a gun which might have been involved in a violent incident, any possible ties relating directly or

indirectly with organized crime, money laundering, or terrorist acts and similar situations. This will be based on a case-by-case situation but will be based on the proper use of both State and Federal laws.

2. Complaints and Corrections

1. If an individual has complaints or objections to the accuracy or completeness of information retained about him or her **within a system under the Center's control**, the Center will inform the individual of the procedure for submitting complaints or requesting corrections. A record will be kept of all complaints and requests for corrections. The procedure submittal will be made in writing and the individual will sign an understanding on his obligation to follow the procedure step-by-step.
2. If an individual has complaints or objections to the accuracy or completeness of information about him or her that **originates with another agency**, the Privacy Office (or CoC while there is no CSO appointed) will notify the originating agency of the complaint or correction request and coordinate with them to ensure that the individual is provided with complaint submission or correction procedures. When the complaint pertains to the correction of a record that has been disclosed to the complainant, the originating agency must consent to the correction, remove the record, or assert a basis for denial. A record will be kept of all complaints and correction requests.
3. If an individual has a complaint with regard to the accuracy or completeness of terrorism-related protected information that:
 - (a) Is exempt from disclosure,
 - (b) Has been or may be shared through the ISE,
 - (c)(i) Is held by the Center and
 - (ii) Allegedly has resulted in demonstrable harm to the complainant,

The center will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the center's Privacy Officer at the following e-mail address: nssic@policia.gov. 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 working 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 by the center of all complaints and the resulting action taken in response to the complaint.

4. To delineate protected information shared through the ISE from other data, the NSSIC maintains records of agencies sharing terrorism-related information and employs system mechanisms to identify the originating agency when the information is shared.
5. If any correction request is denied, to an individual he or she will be given reasons for the rejection. The individual will then be informed of the procedure for appeal when the center or originating agency has declined to correct challenged information to the satisfaction of the individual about whom the information relates.
6. If records that have not been disclosed to a complainant require redressing procedures, the Center will address the issue under applicable law.

F. Security Safeguards

1. The Center Security Officer CSO (or CoC while there is no CSO appointed) will be designated and trained to serve as the center's security officer. The CSO be responsible for all security issues asked of the Center as well as stakeholders and users privileges. He will monitor access privileges; deletion of user id's and reviews of access privileges on a need-to-know basis.
2. The Center will operate in a secure facility protecting the facility from external intrusion, using secure internal and external safeguards against network intrusions. Access to Center databases from outside the facility will only be allowed over secure networks, as the Center will store information in a manner such that it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions.
3. The NSSIC will secure tips, leads, and SAR information in a separate repository system using security procedures and policies that are the same as or similar to those used for a system that secures data rising to the level of reasonable suspicion under 28 CFR Part 23.
4. As previously pointed out, access to the Center's information will only be granted to Center personnel whose position and job duties require such access. These individuals have successfully completed a background check and appropriate security clearance, if applicable, and have been selected, approved, and trained accordingly. Queries made to the Center data applications will be logged into the data system identifying the user initiating the query. The Center will utilize watch logs to maintain audit trails of requested and disseminated information.
5. To prevent public records disclosure, risk and vulnerability assessments will not be stored with publicly available data.

6. The Center will notify an individual about whom personal information was or is reasonably believed to have been breached or obtained by an unauthorized person and access to which threatens the physical, reputational, or financial harm to the person. The notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or any measures necessary to determine the scope of the release of information and, if necessary, to reasonably restore the integrity of any information system affected by this release. The Center will immediately notify the originating agency from which the center received personal information of a suspected or confirmed breach of such information.

G. Information Retention and Destruction

1. All applicable information will be reviewed for record retention (validation or purge) at least every five (5) years, as provided by 28 CFR Part 23. The decision to retain or destroy will be based on whether the information has no further value to the Center's products/Analysts, has not been reviewed in the last five years or meets the criteria for removal according to the Center's retention and destruction policy. If the Center decides information will be removed, it will be purged, destroyed, and deleted or returned to the submitting source. Notification of proposed destruction or return of records will be provided to the contributor, based on agreement with the providing agency. No approval will be required from the originating agency before information held by the Center is destroyed or returned in accordance with this policy or as otherwise agreed upon with the originating agency in a participation or membership agreement.
2. If information collected by the FC will be destroyed, any agency which has received said information will be informed 30 days in advance, in case they want the Center to retain the information as source evidence for an on-going investigation. In that case, an extension of one (1) year will be assigned to the information for future review. If no written notice is received during those 30 days, the information will be automatically destroyed.
3. A record of all these steps will be kept within the Center electronic archives, setting a marker on the date for future review.

H. Information System Transparency, Accountability and Enforcement

1. The Center 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, will be made available upon request, and will be posted online at Homeland Security Information Network page (HSIN). The Privacy Officer (or COC until Privacy Officer is assigned) will be responsible for receiving and responding to

inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s). The Privacy Officer can be contacted at nssic@policia.gov

- 2.
3. Queries made to the Center data applications will be logged into the data system identifying the user initiating the query. The Center's watch log will be utilized to maintain an audit trail of requested or disseminated information for three years.
4. The Center will provide a CD copy of this policy to all agency and non-agency personnel who provide services and will require written acknowledgement of receipt of this policy and agreement of compliance to this policy and the provisions it contains (MOU). The Center will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with their systems, in provisions of this policy and applicable law. This will include logging access of these systems and periodic auditing of these systems, as to not establish a pattern of the audits. These audits will be mandated at least quarterly, and a record of the audit will be maintained by the commander (or designee) of the Center.
5. The Center's personnel or other authorized users shall report violations or suspected violations of Center policies relating to protected information to the Center's privacy officer. The Center will annually conduct internal audits and inspections of the information contained in its criminal intelligence system. In addition, the CEC and CPOC will have the authority to or assign a panel to conduct random audits. This third-party panel has the option of conducting a random audit, without announcement, at any time and without prior notice to the Center. This audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the center's criminal intelligence system.
6. The CPOC (or Privacy Officer) will annually review and update the provisions protecting privacy, civil rights, and civil liberties contained within this policy and make appropriate changes in response to changes in applicable law, changes in technology, changes in the purpose and use of the information systems, and changes in public expectations.
7. The Center will notify an individual about whom sensitive personally identifiable information was or is reasonably believed to have been breached or obtained by an unauthorized person and access to which threatens the physical, reputation, or financial harm to the person. The notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or any measures necessary to determine the scope of the release of information and, if necessary, to reasonably restore the integrity of any information system affected by this release.

8. The Privacy Officer (or COC until Privacy Officer is assigned) ensures that enforcement procedures and sanctions outlined in Section VI, H Information System Transparency, Accountability, and Enforcement are adequate and enforced.
9. Any authorized user found to be not complying with the provisions of this policy regarding the collection, use, retention, destruction, sharing, classification, or disclosure of information will be submitted to any of the following by the Privacy Officer (or COC until Privacy Officer is assigned):
 - Suspension and/or discontinue access to information by the user
 - Suspension, demotion, transfer, or termination of the person, as permitted by applicable personnel policies
 - The application of administrative actions or sanctions as provided by the Center's rules and regulations or as provided in agency personnel policies
 - If the 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
 - And/or refer the matter to appropriate authorities for criminal prosecution, as necessary, to effect the purposes of the policy.
10. The NSSIC 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.

I. Training

1. The Center will require the following individuals to participate in training programs regarding the implementation of and adherence to the privacy, civil rights, and civil liberties policy:
 - All assigned personnel of the center
 - Personnel providing information technology service to the Center
 - Staff in other public agencies or private contractors providing services to the agency,
 - Users who are not employed by the agency or a contractor.
2. The Center will provide special training to personnel authorized to receive, handle, access or share protected information in the Information Sharing Environment regarding the center's requirements and policies for collection, use, and disclosure of protected information.
3. The Center'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

- 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 information accessible within or through the agency
- Mechanisms for reporting violations of center privacy-protection policies
- The nature and possible penalties for policy violations, including suspension or termination of use privileges, discipline sanctions imposed by the user's employing agency, or criminal prosecution
- Originating and participating agency responsibilities and obligations under applicable law and policy.

Appendix A – Terms and Definitions

The following is a list of primary terms and definitions used throughout this template. These terms may also be useful in drafting the definitions section of the fusion center privacy policy.

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. For data access, access is usually specified as read-only access and read/write access.

With regard to the Information Sharing Environment (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 purposes of this definition, acquisition does not refer to the obtaining of information widely available to other ISE participants through, for example, news reports or to the obtaining of information shared with them by another ISE participant who originally acquired the information.

Agency/Center — Agency/Center refers to the Center and all participating state agencies of the Center.

Audit Trail — Audit trail is 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 — Authentication is 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.

Civil Rights — The term “civil rights” is used to imply that the state has a role in ensuring 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 upon 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.

Civil Liberties — Civil liberties are 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.

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

Confidentiality—Confidentiality is 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 or Data—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 acts. The record is maintained in a criminal intelligence system per 28 CFR Part 23. Reasonable suspicion applies to the information. The record is maintained per 28 CFR Part 23.

Data—Inert symbols, signs, or measures.

Data Protection—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, or divulging of personally identifiable information in any other manner—electronic, verbal, or in writing—to an individual, agency, or organization outside of the agency who collected it. Disclosure is a subset 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 disk 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, transmission over the Internet, intranet, extranet, leased lines, dial-up lines, private networks, telephone voice response, and faxback systems. It does not include faxes, telephone calls, video teleconferencing, or messages left on voice mail.

Fair Information Practices — The Fair Information Practices (FIPs) are contained within the Organisation 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 could 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 could 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 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 compound of such data as a given and family name, date of birth, and address. An organization's identification process comprises the acquisition of the relevant identifying information.

Individual Responsibility — Since 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 — 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 three general areas: general data, tips and leads data, and criminal intelligence data.

Information Quality — 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.

Invasion of Privacy — Invasion of privacy can be defined as 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.

ISE-Suspicious Activity Report (ISE-SAR) – An ISE-SAR is a SAR that has been determined, pursuant to a two-part process, to have a potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism). ISE-SAR business, privacy, and civil liberties rules will serve as a unified process to support the reporting, tracking, processing, storage, and retrieval of terrorism-related suspicious activity reports across the ISE.

Law — As used by this policy, law includes any local, state, or federal 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 they are authorized to perform.

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

Maintenance of Information — The maintenance of information applies to all forms of information storage. This would include 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 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 content. 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 upon the type of information and 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.

Non-repudiation— A technique used to ensure that someone performing an action on a computer cannot falsely deny that they performed that action. Non-repudiation provides

undeniable proof that a user took a specific action, such as transferring money, authorizing a purchase, or sending a message.

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

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

Personally Identifiable Information—Personally identifiable information is 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 a United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, 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 — Privacy refers to individuals' interests in preventing the inappropriate collection, use, and release of personally identifiable 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 privacy policy is a written, published statement that articulates the policy position of an organization on how it handles the personally identifiable 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 agency will adhere to those legal requirements and agency 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 agency, the individual, and the public; and promotes public trust.

Privacy Protection — This is a process of finding appropriate balances between privacy and multiple competing interests, such as justice information sharing.

Protected Information —

Protected information includes personal data about individuals and organizations that is subject to information privacy or other legal protections by law, including the U.S. and Puerto Rico constitutions; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 23; and applicable state, local, and tribal laws, ordinances, and codes of Puerto Rico. Protection may be extended to other individuals and organizations by NSSIC policy.

Public — Public includes:

- Any person and any for-profit or nonprofit entity, organization, or association;
- Any governmental entity for which there is no existing specific law authorizing access to the agency's information;
- Media organizations; and
- 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 agency.

Public does not include:

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

Public Access — 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 — Internal procedures to address complaints from persons regarding protected information about them that is under the agency's control.

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 counterterrorism activity.

Right to Privacy — The possible right to be left alone, in the absence of some reasonable public interest in 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 that right.

Role-Based Authorization — a type of 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 — Security refers to the range of administrative, technical, and physical 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.

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.

Sunshine Laws — U.S. federal and state laws requiring regulatory authorities' meetings, decisions and records to be made available to the public.

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 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 or regional fusion center. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor is it designed to support interagency calls for service.

Terrorism Information — Consistent with Section 1016(a)(4) of IRTPA, all information 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 interests of other nations, (C) communications of or by such groups or individuals, or (D) other groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

Terrorism Related Information — In accordance with IRTPA, as recently amended by the 9/11 Commission Act enacted on 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 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 includes intelligence information.

Weapons of Mass Destruction (WMD) information as a fourth (third statutory) category of ISE information is not called for in P.L. 110-53. Rather, it amends the definition of terrorism information to include WMD information and then defines that term. WMD information probably should not, technically, be cited or referenced as a fourth category of information in the ISE.

Tips and Leads Information or Data — Uncorroborated report or information generated from inside or outside the agency that alleges or indicates some form of possible criminal activity. Tips and leads can also be referred to as suspicious incident reports (SIRs), suspicious activity reports (SARs), and/or field interview reports (FIRs). Tips and leads information does not include incidents that do not have an offense attached, criminal history records, or CAD data.

A tip or lead can result from a variety of sources, including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information has some suspicion or mere suspicion attached to it, but without further inquiry or analysis, it is unknown whether the information is accurate or useful. Tips and leads information hangs between being of no use to law enforcement and being extremely valuable if time and resources are available to determine its meaning.

Tips and leads information is maintained in a secure system similar to data that rises to the level of reasonable suspicion.

Appendix B - Federal Laws Relevant to Seeking, Retaining, and Disseminating Justice Information

Excerpt from U.S. Department of Justice's (DOJ) *Privacy, Civil Rights, and Civil Liberties Policy Templates for Justice Information Systems*

The following is a brief listing of federal laws that should be reviewed when developing a privacy policy for a justice information system. The list is arranged in alphabetical order by popular name.

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

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

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

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

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

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

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

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

Electronic Communications Privacy Act of 1986,

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

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

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

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

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

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

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

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

IRTPA, as amended by the 9/11 Commission Act

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

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

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

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

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

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

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

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

USA PATRIOT Act, Public Law No. 107-56
(October 26, 2001), 115 Stat. 272

Appendix C - State Laws Relevant to Seeking, Retaining, and Disseminating Justice Information

Collected from the Lex Juris

The following is a brief listing of state laws that one way or another protects individuals' *privacy, civil rights, and civil liberties* of Individuals under the Commonwealth of Puerto Rico. The list is arranged in alphabetical order by popular name.

Constitution of the Commonwealth of Puerto Rico, Sections 1-20

Letter of Rights of Carriers of the HIV Virus in Puerto Rico, C.C.P.R. § 523, P. de la C. 2980), Law 349, 2000

Record Inspections - Information Access, **Department of Justice, Special Investigations Bureau Law**, C.C.P.R. § 138 I. Title 3 – Executive Power

Protection and Safety of Infants in Hospital Facilities, **C.C.P.R. § 322 Public Policy Declaration**, Title 24 – Health and Hygiene

Organized Crime and Money Laundering Law, **C.C.P.R. § 971q, Judicial Authorization for recording non-telephone conversations**, Title 25 – Internal Security

Civil Rights, **C.C.P.R., Law No. 131 de 13 de mayo de 1943**, as amended; sections 1-6

Elderly Rights Act, C.C.P.R. § 343, Bill of Rights, Title 8 - Public Well Being and Charity Institutions

Well-being and Integral Protection for Childhood Law, Responsibilities and coordination with other agencies, **C.C.P.R. § 444c**

Puerto Rico Penal Code of 1937 and miscellaneous Penal Laws, C.C.P.R. § 2158, Title 33 – Penal Code

Prohibition of Interception of telephone Communications - Inadmissible in Evidence, **Puerto Rico Penal Code of 1937 and miscellaneous Penal Laws**, C.C.P.R. § 2161, Title 33 – Penal Code

Prohibition of Interception of telephone Communications - Penalties, **Puerto Rico Penal Code of 1937 and miscellaneous Penal Laws**, C.C.P.R. § 2162, Title 33 – Penal Code

Illegal Use of Telecommunications - Prohibitions, **Puerto Rico Penal Code of 1937 and miscellaneous Penal Laws**, C.C.P.R. § 2163, Title 33 – Penal Code

Illegal Use of Telecommunications – Manufacture, Possession or Equipment Transfer, **Puerto Rico Penal Code of 1937 and miscellaneous Penal Laws**, C.C.P.R. § 2164, Title 33 – Penal Code

Illegal Use of Telecommunications – Inapplicability of Public Service and Emergency Communications, **Puerto**

Rico Penal Code of 1937 and miscellaneous Penal Laws, C.C.P.R. § 2165, Title 33 – Penal Code

Prohibition of Reproduction, Transfer, Copying, Printing, Banner Use, Publicity and Sale, of Sound Recordings and Live Shows, Puerto Rico Penal Code of 1937 and miscellaneous Penal Laws, C.C.P.R. § 2168, Title 33 – Penal Code

Illegal Collection of Personal Information, Penal Code of 1974, C.C.P.R. § 4182, Title 33 - Penal Code

Written Communication Privacy Violation, Penal Code of 1974, C.C.P.R. § 4184, Title 33- Penal Code

Interception of Verbal Private Communication, Penal Code of 1974, C.C.P.R. § 4185, Title 33 - Penal Code

Recording, Penal Code of 1974, C.C.P.R. § 4186, Title 33- Penal Code

Disclosure of Private Conversation, Penal Code of 1974, C.C.P.R. § 4187, Title 33 - Penal Code

Private Conversation Publishing, Penal Code of 1974, C.C.P.R. § 4188, Title 33 - Penal Code

Message Alteration, Penal Code of 1974, C.C.P.R. § 4189, Title 33 - Penal Code

Improper Private Communication Usage, Penal Code of 1974, C.C.P.R. § 4190, Title 33 - Penal Code

Serious crimes, Penal Code of 1974, C.C.P.R. § 4191, Title 33 - Penal Code

Disclosure of Professional Secrets, Penal Code of 1974, C.C.P.R. § 4192, Title 33 – Penal Code

Personal Tranquility Intrusion, Penal Code of 1974, C.C.P.R. § 4193, Title 33 – Penal Code

Fraudulent Interference with counters or communication equipment, Penal Code of 1974, C.C.P.R. § 4275, Title 33 – Penal code

Wired communication Fraud, Penal Code of 1974, C.C.P.R. § 4275b, Title 33 – Penal Code

Alteration, Damage or Destruction of Computers, Penal Code of 1974, C.C.P.R. § 4275c, Title 33 – Penal Code



Kansas Intelligence Fusion Center

Privacy Policy

As Adopted by the Fusion Center Oversight Board

Adopted June 26, 2020

This page intentionally left blank.

Kansas Intelligence Fusion Center Privacy Policy

Table of Contents

I.	Mission/Purpose.....	5
II.	Policy Applicability and Legal Compliance	5
III.	Governance and Oversight.....	6
IV.	Information	6
V.	Acquiring and Receiving Information	10
VI.	Information Quality Assurance.....	11
VII.	Collation and Analysis	12
VIII.	Merging Records.....	12
IX.	Sharing and Disclosure	13
X.	Redress.....	15
XI.	Security	16
XII.	Information Retention and Destruction	17
XIII.	Accountability and Enforcement	18
XIV.	Training.....	19
	APPENDIX A (User Agreement)	21
	APPENDIX B (Terms and Definitions)	23
	APPENDIX C (Markings and Classification)	34
	APPENDIX D (References)	36

This page intentionally left blank.

I. Mission/Purpose

The mission of the Kansas Intelligence Fusion Center (KIFC) is to protect the people and property of Kansas by providing a multi-discipline, information sharing network designed to gather, analyze, and disseminate information to public and private stakeholders in a timely manner and consistent with the privacy rights of our citizens.

The KIFC is tasked with implementing a collaborative effort to assemble, collate, analyze, and disseminate information to appropriate agencies and individuals, in an effort to mitigate terrorist and criminal related activities. Equally important is KIFC's commitment to safeguard the privacy, civil rights, and civil liberties of U.S. citizens. This detailed policy documents those efforts.

II. Policy Applicability and Legal Compliance

All KIFC personnel, whether full, part-time, or temporarily assigned, employed by the KIFC or by partner agencies, will be trained in and comply with this policy. The KIFC has adopted internal operating policies that are in compliance with applicable law protecting privacy, civil rights, and civil liberties, including, but not limited to federal and state laws listed in Appendix D. Agencies and individual users of KIFC work products are also required to comply with applicable sections of this policy. Additional notifications of that requirement will be made as appropriate, by an attachment to individual work products. All KIFC personnel and participating agencies will comply with this privacy policy concerning the information the KIFC collects, receives, maintains, archives, accesses, or discloses to KIFC personnel, government agencies, including Information Sharing Environment (ISE) participating agencies, and participating law enforcement and public safety, as well as to private sector/critical infrastructure participants, private contractors and the general public.

All KIFC personnel, participating agency personnel, personnel providing information technology services to the agency, private contractors, private sector/critical infrastructure participants and other authorized users will be directed to review and comply with this policy and will comply with all federal and state privacy, civil rights, and civil liberties law cited in Appendix D of this policy. The KIFC will provide a printed copy of this policy to all personnel performing duties in the KIFC including: participating agency personnel, personnel providing information technology services to the agency, private contractors, private sector/critical infrastructure participants and other authorized 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. This agreement is contained in APPENDIX A of this document.

KIFC will make a copy of this policy available to any interested party, public or private. See Section XIII.

III. Governance and Oversight

The KIFC is multi-agency/multi-discipline collaborative initiative operated and administered pursuant to state and federal law. Primary responsibility for the operation of the KIFC operations, and coordination of personnel; the receiving, seeking, retention, evaluation, information, quality, analysis, destruction, sharing, and disclosure of information, and the enforcement of this policy is assigned to the Executive Director of the KIFC as designated by the Fusion Center Oversight Board (Board). Operation and management of law enforcement systems, or data/information systems used by other participating agencies, will be the responsibility of those agencies and their assigned representatives in the KIFC.

The KIFC is governed by the Board whose membership is established by K.S.A. 2018 Supp. 48-3701 through 48-3710. Each member has an equal vote on all matters before the Board except where otherwise established by statute. The Board strives 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 Board will periodically review and update the policy in response to changes in law and implementation experience, including the results of audits and inspections.

As the Chair of the Board, the Kansas Attorney General (AG) has designated a senior attorney within the Office of the Attorney General to serve as privacy and civil liberties counsel (Privacy Counsel) to the KIFC. The Privacy Counsel works with the Executive Director to ensure all KIFC analysis and operations comply with all applicable federal and state privacy or civil liberties laws and obligations. The Privacy Counsel receives reports regarding alleged errors and violations of the provisions of this policy, receives and coordinates complaint resolution under the center's redress policy, and serves as the liaison for the Information Sharing Environment, ensuring that privacy protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy-enhancing technologies. The Privacy Counsel ensures that enforcement procedures and sanctions outlined in Section XIII., *Accountability and Enforcement* are adequate and enforced. The Privacy Counsel, Deputy Attorney General Jay Scott Emler, can be contacted at the following address: jay.emler@ag.ks.gov.

As appropriate, the Board, the Executive Director or the Privacy Counsel will, when necessary, interact with privacy advocacy groups to address issues regarding the KIFC's information collection, retention, and dissemination processes.

For examples of primary terms and definitions used in this policy, refer to Appendix B, Terms and Definitions.

IV. Information

In fulfilling its public safety role, the KIFC may actively seek, analyze, disseminate, and retain information that is based on terrorism, asymmetric threat or international criminal enterprise

related criminal predicates, a reasonably suspected terrorism nexus, or which negatively impacts on public safety. Such information must be believed to be relevant to investigation, prosecution, or predictive analysis serving the prevention of genuine public safety threats or the mitigation of genuine public safety incidents. In order to provide law enforcement, public safety and other affected agencies with actionable intelligence, the KIFC may also engage in research toward that end. All KIFC employees will ensure that information (including information sources as applicable) is verifiable (to include coordinating with originating agencies to determine if their information is reliable and verifiable as described in Section VI), collected in a lawful manner, and lawfully disseminated. Only KIFC staff and analysts, participating agency analysts, vetted and approved contractors, and other pre-authorized personnel will be able to access the information. The limitations on the quality of the information will be noted if a source is of doubtful credibility and as provided in Section VI., *Data Quality*. KIFC may retain preliminary information such as tips and leads, and suspicious activity reports (SAR), providing the information is arguably of public safety interest. Whenever possible, data regarding criminal investigations will reside on or be entered into existing law enforcement systems used and administered by participating agencies.

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 SAR information, subject to the conditions and procedures specified in this policy. The KIFC 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, citizenships, places of origin, ages, disabilities, genders, or sexual orientations. Information will be disseminated to individuals based on “need to know” and “right to know” (See definitions in Appendix B).

The KIFC applies labels to KIFC-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 in Appendix B, to include personal data on any individual and, to the extent expressly provided in this policy, includes organizational entities.
- The information is subject to Chapter 45 of Kansas Statutes Annotated (included in APPENDIX D of this policy), restricting access, use, or disclosure.

The KIFC personnel will ensure certain basic descriptive information (metadata tags or labels) is entered and associated with data for which there are specific laws, rules, or policies regarding access, use, and disclosure including terrorism-related information shared through the ISE. The types of information that will be included are: the name of the originating department, component, and subcomponent; the name of the agency or department’s law enforcement information system where the information was obtained; the date the information was collected, and when available, the date its accuracy was last verified; the title and contact information for the person who provided the information; and the person to whom future questions regarding the information can be directed. KIFC personnel will ensure that specific labels and metadata have been applied to the information that will be used, accessed, and disseminated to clearly indicate any legal restrictions on information sharing based on information sensitivity or classification.

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

- Protect confidential sources and police undercover techniques and methods.
- Not interfere with or compromise pending criminal investigations.
- Protect an individual's right of privacy or his or her civil rights and civil liberties.
- Provide legally required protections based on the individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.

Information received, analyzed, and disseminated at the KIFC will include, at a minimum, indicators for type of criminal investigation, tips and leads, source information, requestor identification, reliability of the source and validity of the content, sensitivity, juvenile information, and protected status information. The KIFC will identify and review protected information that may be accessed from or disseminated by the KIFC 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, which will enable ISE authorized users to determine the nature of the protected information and how to handle the information in accordance with applicable legal requirements. No information, specifically provided to the KIFC, will be disseminated to a third party without the consent of the information's originating agency. Only the original classifying authority may authorize dissemination of or downgrade of classified material.

During receipt, storage, or dissemination of information, KIFC personnel will assess the information for sensitivity, evaluate to determine its credibility, label the information as either unsubstantiated/uncorroborated if the validation or reliability is uncertain, and document the information received/disseminated. All information obtained from outside agencies with a sensitivity label will be evaluated by KIFC personnel and relabeled with the same labels used by KIFC personnel. The original label will be maintained with the information. All information will be labeled as Unclassified, Controlled Unclassified Information, For Official Use Only, Law Enforcement Sensitive or the appropriate marking for classified information. See APPENDIX B, Definitions for further information.

The labels assigned to existing information under Section V 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.
- New information is added that would increase/decrease the classification of disclosure.

The KIFC will keep a record of the source of all information sought, collected, and retained by the agency. Tips and Leads information will be clearly labeled as such and be retained long enough to validate the source and reliability of the information. Tips and Leads information will

be afforded the same level of physical and technical security as that given to information containing reasonable suspicion.

SAR Specific

KIFC 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. KIFC 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 which rises to the level of reasonable suspicion and which includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information.
- Allow access to or disseminate the information using the same (or a more restrictive) access or dissemination standard that is used for data that rises to the level of reasonable suspicion (for example, “need-to-know” and “right-to-know” access or dissemination for personally identifiable information).
- Regularly provide access to or disseminate the information in response to an interagency inquiry for law enforcement, homeland security, or public safety and analytical purposes or provide an assessment of the information to any agency, entity, individual, or the public when credible information indicates potential imminent danger to life or property.
- Retain information for 2 years in order to work an unvalidated tip, lead, or SAR information to determine its credibility and value or assign a “disposition” label (for example, undetermined or unresolved, cleared or unfounded, verified, or under active investigation) so that a subsequently authorized user knows the status and purpose for the retention and will retain the information based on the retention period associated with the disposition label.
- Adhere to and follow the center’s physical, administrative, and technical security measures to ensure the protection and security of tips, leads, and SAR information. Tips, leads, and SAR information will be secured in a system that is the same as or similar to the system that secures data that rises to the level of reasonable suspicion.

The KIFC 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.

All KIFC analytical products will be reviewed, as appropriate, by the KIFC Privacy Officer prior to dissemination.

V. Acquiring and Receiving Information

Information gathering, including acquisition and access, and investigative techniques used by the KIFC and information-originating agencies are in compliance with and will adhere to applicable regulations and guidelines, including, but not limited to:

- 28 CFR Part 23 regarding criminal intelligence information (APPENDIX D)
- Organization for Economic Co-operation and Development's (OECD) Fair Information Practices (under certain circumstances, there may be exceptions to the Fair Information Practices, based, for example, on authorities paralleling those provided in the Federal Privacy Act; state, local, and tribal laws, or KIFC policy)
- Applicable criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) National Criminal Intelligence Sharing Plan NCISP)
- Applicable constitutional provisions, Chapter 45 of Kansas Statute Annotated [Kansas Open Records Act (KORA) and Kansas Open Meetings Act (KOMA)], and the applicable administrative rules, as well as any other regulations that apply to multijurisdictional intelligence databases.

SAR Specific

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

The KIFC's SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals or organizations 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 (e.g. race, religion, national origin, and ethnicity) and civil liberties (e.g. speech, assembly, and religious exercise) will not be intentionally or inadvertently gathered, documented, processed, and shared.

In providing information, KIFC contributors are governed by the laws and rules of their individual agencies, as well as by applicable state and federal laws restricting access, use, or disclosure. External agencies that access the KIFC'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 KIFC will not directly or indirectly receive, seek, accept, or retain information from:

- An individual who or nongovernmental entity that may or may not receive a fee or benefit for providing the information, except as expressly authorized by law or KIFC policy.
- An individual who or information provider that is legally prohibited from obtaining or disclosing the information.

A human review of the information ensures the information was gathered legally and ensures all information that is disseminated or shared through the ISE does not violate civil rights or civil

liberties. If there is suspicion that information was illegally obtained it should be reported to the KIFC Privacy Officer.

Information gathering and investigative techniques used by the KIFC will (and from the originating agencies should) be the least intrusive means necessary in the particular circumstances to gather information it is authorized to seek or retain. The KIFC will contract only with commercial database entities that provide an assurance that their methods for gathering personally identifiable information (PII) comply with applicable local, state, tribal, territorial, and federal laws, statutes, and regulations and that those methods are not based on misleading information collection practices.

Any further information regarding processes and day-to-day operations can be found in the numerous duty and software manuals used by and within the KIFC. These manuals will not be available to the general public because of sensitivity issues involving the release of security information.

VI. Information Quality Assurance

The KIFC will make reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources. Further, the KIFC will make reasonable effort to ensure the information is 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 has been met [Refer to Section VIII Merging Records]. The KIFC investigates, in a timely manner, alleged errors and deficiencies and corrects, deletes, or refrains from using protected information found to be erroneous or deficient.

At the time of retention in the system, the information will be labeled regarding its level of quality (accurate, complete, current, verifiable, and reliable). For further information refer to KIFC Policies and Procedures manual. The labeling of retained information will be reevaluated when new information is gathered that has an impact on the validity and reliability of retained information.

The KIFC will conduct periodic data quality reviews of information it originates and make every reasonable effort to ensure the information will be corrected, deleted from the system, or not used when the KIFC identifies information that is erroneous, misleading, obsolete, or otherwise unreliable; the KIFC did not have authority to gather the information or to provide the information to another agency; or the KIFC used prohibited means to gather the information (except when the KIFC's information source did not act as the agent of the KIFC in gathering the information).

Originating agencies external to the KIFC are responsible for reviewing the quality and accuracy of the data provided to the KIFC. The KIFC 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 KIFC will use written or electronic notification to inform recipient agencies when information previously provided to the recipient agency is deleted or changed by the KIFC 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

All KIFC Intelligence Analysts have successfully passed a background check, possess an appropriate security clearance, and have been selected, approved, and trained according to KIFC requirements. They are authorized to seek, accept, retain, and disseminate appropriate information. Such information undergoes analysis in order to enhance public safety, assist in investigations and prosecutions, and provide tactical and strategic intelligence services to authorized recipients.

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

Information acquired or received by the KIFC is analyzed according to priorities and needs and will be analyzed only to:

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

The KIFC requires that all analytical products be reviewed by the KIFC Director and by the KIFC Privacy Officer to ensure such products provide appropriate privacy, civil rights, and civil liberties protections prior to dissemination or sharing by the center.

VIII. Merging Records

If, during analysis, information from disparate sources regarding an individual or organization is determined to be of such validity and quantity to lead a reasonable person to conclude that the individuals or organizations are one in the same, an analyst may merge the information within KIFC work products and records. The set of identifiers sufficient to allow merging will consist of all available attributes that can contribute to a higher accuracy of match. In such an instance, the contributing and recipient agency will be notified of the merger. No alterations or modifications will be made by KIFC personnel to a contributing, participating, or recipient agency's data systems, unless that KIFC analyst is an authorized representative of that participating agency and has been granted the required administrative privileges to correct or update data in that agencies system.

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

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

IX. Sharing and Disclosure

Credentialed, role-based access criteria will be used, 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; and
- To whom, individually, the information can be disclosed and under what circumstances.

The KIFC adheres to the current version of the ISE-SAR Functional Standard for its SAR reporting 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 KIFC will be provided only *to persons within the KIFC or in other governmental agencies* who are authorized to have access and only for legitimate law enforcement, public protection, public prosecution, public health, or justice purposes and only for the performance of official duties in accordance with law and procedures applicable to the agency for which the person is working. KIFC will obtain authorization from originating agencies or original classifying authority prior to disseminating to third parties information specifically supplied to the KIFC. An audit trail sufficient to allow the identification of each individual who accessed information retained by the KIFC and the nature of the information accessed will be kept by the KIFC. Agencies external to the KIFC may not disseminate information accessed or disseminated from the KIFC without approval from the KIFC or other originator of the information.

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

Information gathered or collected and records retained by the KIFC 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 KIFC; the nature of the information requested, accessed, or received; and the specific purpose will be kept for a minimum of 5 years by the KIFC.

Information gathered or collected and records retained by the KIFC 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 KIFC'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 KIFC for such of information. Information that is considered open-source or public record may be released outside the public safety community if such disclosure will further the KIFC mission and the recipient has a valid "need to know." An audit trail sufficient to allow the identification of each individual member of the public who accessed or received information retained by the KIFC and the nature of the information accessed will be kept by the KIFC.

Information gathered or collected and records retained by the KIFC *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.

Permission to distribute any information to any person or organization will be sought from the owner of that information before any release, unless that information is obtained from open sources available to anyone in the public or prior approval has been granted. Organizations external to the KIFC may not disseminate KIFC information received from KIFC without approval from the originator of the information.

Certain other records will not be disclosed to the public, including but not limited to:

- Records required to be kept confidential by law are exempt from disclosure requirements under KORA (KSA 45-221(a)(1)).
- Information that meets the definition of "classified information" as that term is defined in the National Security Act, Public Law 235, Section 606, and in accordance with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010.
- Investigatory records of law enforcement agencies are exempt from disclosure requirements under KORA. However, certain law enforcement records must be made available for inspection and copying under KORA (KSA 45-221 (a)(10)).
- 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 exempt from disclosure requirements under Chapter 45 of Kansas Statute Annotated. This includes a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism under Chapter 45 of Kansas Statute Annotated or an act of agricultural terrorism under Chapter 45 of Kansas Statute Annotated, vulnerability assessments, risk planning documents, needs assessments, and threat assessments (KSA 45-221(a)(45)).

The KIFC 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

Upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity and subject to the conditions specified in the following paragraph, an individual is entitled to know the existence of and to review the information about him or her that has been gathered and retained by the KIFC. Access to this information will be processed by and provided by the KIFC Privacy Officer. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information (correction). The KIFC'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. For the purpose of creating an audit trail, a record of all requests for access to information will be kept for a minimum of five (5) years and shall include what information is disseminated to each person in response to the request. This process will be followed for all requests.

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

- Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution per exemptions from disclosure requirements under, but not limited to, Chapter 45 of Kansas Statutes Annotated (KSA 45-221 (a)(10)).
- Disclosure would endanger the health or safety of an individual, organization, or community per exemptions from disclosure requirements under, but not limited to, Chapter 45 of Kansas Statutes Annotated (KSA 45-221 (a)(45)).
- The information is in a criminal intelligence information system subject to 28 CFR Part 23 [see 28 CFR § 23.20(e)].
- The information disclosure would have a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack and is exempt from disclosure requirements under Chapter 45 of Kansas Statutes Annotated. This includes a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism under Chapter 45 of Kansas Statute Annotated or an act of agricultural terrorism under Chapter 45 of Kansas Statute Annotated, vulnerability assessments, risk planning documents, needs assessments, and threat assessments.

If the information does not originate with the KIFC, the requestor will be referred to the originating agency, if appropriate or required by law. In the event the KIFC determines referral is neither appropriate nor required, the KIFC will notify the source agency of the request and of the KIFC's determination that disclosure **by the KIFC** or referral **of the requestor** to the source agency was neither required nor appropriate under applicable law. Final approval of dissemination shall rest with the KIFC Director.

If an individual requests correction of information *originating with the KIFC* that has been disclosed, the KIFC'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.

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 KIFC or the originating

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

If an individual has a complaint with regard to the accuracy or completeness of terrorism-related protected information that: (1) Is exempt from disclosure, (2) has been or may be shared through the ISE, (3) is held by the KIFC and (4) allegedly has resulted in demonstrable harm to the complainant, the center will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the KIFC's Privacy Counsel, Deputy Attorney General Jay Scott Emler at the following address: jay.emler@ag.ks.gov. The Privacy Counsel 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 KIFC, the Privacy Counsel 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 KIFC that is the subject of a complaint will be reviewed within 30 days and confirmed or corrected/purged if determined to be out of date, inaccurate or incomplete, to include incorrectly merged information. If there is no resolution within 30 days, the KIFC will not share the information until such time as the complaint has been resolved. A record will be kept by the KIFC 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 KIFC maintains records of agencies sharing terrorism-related information and employs system mechanisms to identify the originating agency when the information is shared.

XI. Security

The KIFC is an authorized tenant organization (at the discretion of The Adjutant General-Kansas/Kansas Homeland Security Director) within a Secure Facility that is operated, secured and maintained (including Defense Intelligence Agency Accreditation) by the Kansas National Guard. The Kansas National Guard provides a Special Security Officer (SSO) who will be designated as the KIFC's security officer and will ensure the center operates in a secure manner free from facility and network intrusion. The designated security officer will attend training through a federally approved program. The KIFC will operate in this secure facility protected from external intrusion. The KIFC will utilize secure internal and external safeguards against network intrusions. Access to the KIFC's databases from outside the facility will be allowed only over secure networks.

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

Access to KIFC information will be granted only to KIFC personnel whose positions and job

duties require such access; who have successfully completed a background check and received an appropriate security clearance, if applicable; and who have been selected, approved, and trained accordingly. Queries made to the KIFC's data applications will be logged into the data system identifying the user initiating the query. The KIFC will utilize watch logs 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 KIFC will notify an individual about whom personal information was or is reasonably believed to have been breached or obtained by an unauthorized person and access to which threatens physical, reputational, or financial harm to the person. The notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or any measures necessary to determine the scope of the release of information and, if necessary, to reasonably restore the integrity of any information system affected by such release and provided that notification does not compromise an ongoing investigation. The Board will also be notified and a determination made as to whether additional investigative assistance is required. If the security breach was directed toward KIFC Databases and/or Information Systems, personnel from all concerned or potentially impacted agencies will be notified.

KIFC personnel are required to secure ongoing work products within their workspaces at the end of any shift. Wall postings that could possibly compromise the integrity of any investigation or inadvertently reveal personal information should be secured. Visitors through the KIFC must provide adequate identification and a valid need to visit, and any maintenance personnel must be escorted. All visitors to the KIFC must be approved in advance by the SSO office, unless emergency circumstances preclude advanced notification.

XII. Information Retention and Destruction

All applicable information will be reviewed for record retention (validation or purge) by the KIFC 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 KIFC's retention and destruction policy, it will be purged, destroyed, and deleted or returned to the submitting (originating) agency. The KIFC 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 KIFC 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 KIFC, depending on the relevance of the information and any agreement with the originating agency. A record of information to be reviewed for retention will be maintained by the KIFC, and for appropriate system(s), notice will be given to the submitter at least 30 days prior to the required review and validation/purge date.

Exact processes for purging and destroying information are stated in the KIFC Policies and Procedures manual.

XIII. Accountability and Enforcement

The KIFC will be open with the public in regard to information and intelligence collection practices. The KIFC's privacy policy will be provided to the public for review and made available upon request by email to the KIFC Privacy Officer, Deputy Attorney General Jay Scott Emler, at jay.emler@ag.ks.gov. The privacy policy (or a notice of its availability and the process for requesting a copy of the policy provided) will be posted on the KIFC website once it has been completed and URL is available. The KIFC's Privacy Officer will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s) maintained or accessed by the center. The Privacy Officer, Deputy Attorney General Jay Scott Emler, can be contacted at the following address: jay.emler@ag.ks.gov.

The audit log of queries made to the KIFC will identify the user initiating the query. The KIFC will maintain an audit trail of accessed, requested, or disseminated information. An audit trail will be kept for a minimum of 5 years of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.

The KIFC 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 random 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 KIFC. The KIFC's personnel or other authorized users shall report errors and suspected or confirmed violations of KIFC policies relating to protected information to the KIFC's Privacy Officer.

The KIFC will annually conduct an audit and inspection of the information and intelligence contained in its information system(s). The audit will be conducted by the KIFC's Board, guided by the Privacy Officer. The Board has the option of conducting a random audit, without announcement, at any time and without prior notice to staff of the KIFC. The audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the KIFC's information and intelligence system(s).

The Board, 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.

If KIFC 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 KIFC Director will:

- Suspend or discontinue access to information by such KIFC personnel, the participating agency, or the authorized user.
- Suspend, demote, transfer, or terminate KIFC personnel, as permitted by applicable personnel policies.
- Apply administrative actions or sanctions as provided by applicable KIFC rules and

regulations or as provided in KIFC personnel policies.

- If the authorized user is not a KIFC employee, request the relevant agency, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions.
- Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

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

XIV. Training

The KIFC 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 assigned personnel of the KIFC.
- Personnel providing information technology services to the KIFC.
- Staff in other public agencies or private contractors providing services to the KIFC.
- Users who are not employed by the KIFC or a contractor.

The KIFC will provide special training regarding the KIFC's requirements and policies for collection, use, and disclosure of protected information to personnel authorized to share protected information through the ISE.

The KIFC'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 KIFC.
- 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 the KIFC.
- Mechanisms for reporting violations of KIFC 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

User Agreement



**Kansas Intelligence Fusion Center (KIFC)
Privacy, Civil Liberties, and Civil Rights Policy**

POLICY NOTE

This policy does not constitute a contract of any kind. The Fusion Center Oversight Board, the KIFC Executive Director, and the KIFC Privacy Counsel reserve the right to change the policy at any time, without any advance notice. A copy of the most current policy will be provided to all employees and others working in the KIFC.

This policy document was approved via electronic communication and comment by the KIFC Privacy Counsel on the ____ day of _____, 2019.

Jared Hartter
Executive Director, KIFC

EMPLOYEE/CONTRACTOR/VENDOR PRIVACY, CIVIL LIBERTIES, AND CIVIL RIGHTS POLICY ACKNOWLEDGMENT:

I hereby acknowledge that I have received a copy of the KIFC Privacy Policy and have read it in its entirety. I agree with and will comply with all of its provisions terms.

Employee/Contractor/Vendor Signature

Date

Printed Name

Company/Organization Name – (non-KIFC)

APPENDIX B

Terms and Definitions

The following is a list of primary terms and definitions used throughout this policy. These terms are useful in understanding the meaning of terms within in this policy.

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. For data access, access is usually specified as read-only access 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 homeland security information, terrorism information, and law enforcement information acquired in the first instance by another ISE participant.

Audit Trail—Audit trail is 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, including but not limited to what commands were issued to the system, and what records and files were accessed or modified.

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

Authorization—The process of granting a person, computer process, or device 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.

Civil Rights—The term “civil rights” is used to imply that the state has a role in ensuring all citizens have equal protection under the law and equal opportunity to exercise the rights of citizenship regardless of race, religion, gender, or other characteristics unrelated to the worth of the individual. Civil rights are, therefore, obligations imposed upon 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.

Civil Liberties—Civil liberties are 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.

Classified Information— means any information or material that has been determined by the United States Government pursuant to an Executive order, statute, or regulation, to require protection against unauthorized disclosure for reasons of national security and any restricted data, as defined in paragraph r. of section 11 of the Atomic Energy Act of 1954 (42 U.S.C. 2014 (y)). Pursuant to Executive Order 12356, the three levels of classification are “top secret,” “secret” and “confidential.”

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

Confidentiality—Confidentiality is 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.

Controlled Unclassified Information (CUI) — the categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is:

- pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government
- under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination

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.

Data—Inert symbols, signs, or measures.

Disclosure—The release, transfer, provision of access to, or divulging of personally identifiable information in any manner, including but not limited to, electronic, verbal, or written, to an individual, agency, or organization outside of the agency that collected it. Disclosure is a subset of privacy, focusing on information that may be available only to certain people for certain purposes, but that is not available to everyone.

Fair Information Practices—The Fair Information Practices (FIPs) are contained within the Organization for Economic Cooperation and Development’s (OECD) Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data. These were developed around commercial transactions and the Trans-Border 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

Homeland Security Information—As defined in Section 482(f)(1) of the Homeland Security Act, homeland security information 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.

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 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 compound of such data as a given and family name, date of birth, and address. An organization's identification process comprises the acquisition of the relevant identifying information.

Information—Information includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists. Information received by law enforcement agencies can be categorized into four general areas: general data, investigatory work product, tips and leads data, and criminal intelligence data.

Information Quality—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.

Kansas Intelligence Fusion Center (KIFC) —The KIFC is the state designated fusion center for the state of Kansas and brings local, state and federal law enforcement officials together with public and private organizations to detect, deter and respond to terrorist threats in Kansas.

Law—As used by this policy, law includes any local, state, or federal 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.

Logs—Logs are a generic term for recording (logging) a sequence of activities. In computer and network contexts, logs track the sequence of activities on a system, such as user log-ins and log-outs—See also Audit Trail.

Metadata—In its simplest form, metadata is information (data) about information, more specifically information about a particular content. 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 upon the type of information and 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.

Permission(s)—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 Data—Personal data refers to any personally identifiable information that relates to an identifiable individual (or data subject). See also Personally Identifiable Information.

Personally Identifiable Information—Personally identifiable information is one or more pieces of information that when considered together or when considered in the context of how it is presented or how it is gathered is 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 a United States citizen, an alien known by the intelligence agency considered to be a permanent resident alien, 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 State citizens and lawful permanent residents.

Privacy—Privacy refers to individuals’ interests in preventing the inappropriate collection, use, and release of personally identifiable 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 privacy policy is a written, published statement that articulates the policy position of an organization on how it handles the personally identifiable 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 agency will adhere to those legal requirements and agency 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 agency, the individual, and the public; and promotes public trust.

Privacy Protection—This is a process of finding appropriate balances between privacy and multiple competing interests, such as justice information sharing.

Protected Information—includes Personal Data about individuals that is subject to information privacy or other legal protections under the U.S. Constitution and the Kansas constitution; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 23; applicable state and tribal constitutions; and State, Local and Tribal laws, ordinances, and codes.

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 agency’s information;

- Media organizations; and
- 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 agency.

Public does not include:

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

Public Access—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—Internal procedures to address complaints from persons regarding protected information about them that is under the agency’s control.

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 counterterrorism activity.

Security—Security refers to the range of administrative, technical, and physical 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.

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 homeland security information, terrorism information, and law enforcement information by both the originator of the information and any recipient of the information.

Suspicious Activity—Suspicious activity is defined as “behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal espionage, or other illicit intention. Examples of suspicious activity include, but are not limited to: surveillance, photography of facilities, site breach or physical intrusion, cyber attacks, testing of security.

Suspicious Activity Reports (SAR)—The observation and documentation of a suspicious activity. SARs are meant to offer a standardized means for feeding information repositories or data mining tools. Any patterns identified during SAR data mining and analysis may be investigated in coordination with the reporting agency and the state designated fusion center. The SAR is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities. Nor are they designed to support interagency calls for service.

Terrorism-Related Information—In accordance with IRTPA, as recently amended by the 9/11 Commission Act enacted on 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 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 includes intelligence information.

Weapons of Mass Destruction (WMD) information as a fourth (third statutory) category of ISE information is not called for in P.L. 110-53. Rather, it amends the definition of terrorism information to include WMD information and then defines that term. WMD information probably should not, technically, be cited or referenced as a fourth category of information in the ISE.

Tips and Leads Information—Uncorroborated report or information generated from inside or outside the agency that alleges or indicates some form of possible criminal activity. Tips and leads can also be referred to as suspicious incident reports (SIRs), SARs, and/or field interview reports (FIRs). Tips and leads information does not include incidents that do not have an offense attached, criminal history records, or CAD data.

A tip or lead can result from a variety of sources, including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information has some suspicion or mere suspicion attached to it, but has not been evaluated and vetted.

Tips and leads information is maintained in a secure system similar to data that rises to the level of reasonable suspicion.

APPENDIX C

Markings and Classification

Unclassified Documents will be marked as follows:

Open Source Information that can be obtained legally by request, purchase, or observation. This information will be marked as “Unclassified” if assemble in KIFC products.

Controlled Unclassified Information (CUI): Categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is:

- Pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government
- Under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination
- Includes categories such as For Official Use Only (FOUO), Law Enforcement Sensitive (LES), and Sensitive But Unclassified (SBU).

All CUI will maintain original markings when stored or integrated into KIFC products.

Protected Critical Infrastructure Information (PCII)

- Only the PCII Program Office or a PCII Program Manager Designee may mark information as PCII and provide it with a submission identification number. Information that does not contain the requisite PCII markings and identification number is not PCII. The PCII marking remains until the PCII Program Office determines that the information no longer qualifies for PCII protection or the submitter requests that the protection be removed.
- PCII Authorized Users must ensure products created from PCII include a PCII coversheet and are marked with “Protected Critical Infrastructure Information” in the headers and footers to alert users to the information’s status and protection requirements.

All other Unclassified Documents will be marked appropriately per guidance from originating authority.

Classified Information will be marked as follows:

All Classified information will be marked in accordance with Executive Order 12958, as amended and ISOO Implementing Directive No. 1 that prescribes a uniform security classification system for Classified National Security Information.

APPENDIX D

References: Applicable State and Federal Laws and Regulations

Excerpt from

*U.S. Department of Justice's (DOJ's) Privacy, Civil Rights, and Civil Liberties
Policy Templates for Justice Information Systems*

The U.S. Constitution is known as the primary authority that applies to federal as well as state, local, and tribal (SLT) agencies. State constitutions cannot provide fewer privacy and other civil liberties protections than the U.S. Constitution but can (and many do) provide enhanced privacy and other civil liberties protections.

Civil liberties protections are primarily founded in the Bill of Rights. They include the basic freedoms, such as free speech, assembly, and religion; freedom from unreasonable search and seizure; due process; etc. The relationship of these fundamental rights to the protection of privacy, civil rights, and other civil liberties in the Information Sharing Environment is explored in a key issues guidance paper titled *Civil Rights and Civil Liberties Protection*, which is available on the Program Manager (PM) for the Information Sharing Environment (PM-ISE) Web site at www.isc.gov.

Statutory civil rights protections in the U.S. Constitution may, in addition, directly govern state action. These include the Civil Rights Act of 1964, as amended; the Rehabilitation Act of 1973; the Equal Educational Opportunities Act of 1974; the Americans with Disabilities Act; the Fair Housing Act; the Voting Rights Act of 1965; and the Civil Rights of Institutionalized Persons Act.

Federal laws, Executive Orders, regulations, and policies directly affect agencies'/centers' privacy policies. While SLT agencies may not be generally bound directly by most statutory federal privacy and other civil liberties protection laws in the information collection sharing context, compliance may be required **indirectly** by funding conditions (e.g., 28 CFR Parts 20, 22, and 23 or the Health Insurance Portability and Accountability Act [HIPAA]); operation of the Commerce Clause of the U.S. Constitution (e.g., Electronic Communications Privacy Act of 1986); or a binding agreement between a federal agency and an SLT agency (e.g., a memorandum of agreement or memorandum of understanding). Where relevant or possibly relevant, agencies/centers are advised to list these laws, regulations, and policies, noting those that may potentially affect the sharing of information, including sharing terrorism-related information in the Information Sharing Environment.

The development of a privacy, civil rights, and civil liberties policy is primarily designed for center personnel and authorized users to ensure that they are aware of the legal and privacy

framework within which they and the center must operate. If the applicability and requirements of various laws, regulations, or sharing agreements are not spelled out or referenced in a center privacy policy, staff and user accountability is greatly diminished, mistakes are made, privacy violations occur, and the public's (and other agencies') confidence in the ability of the center to protect information and intelligence is compromised. When staff members know the rules through sound policy and procedure communicated through ongoing training activity, information sharing is enhanced.

Following is a partial listing of federal laws that should be reviewed when developing a privacy policy for a justice information system. The list is arranged in alphabetical order by popular name.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Reference:
Executive Order 12333
United States Intelligence Activities

(As amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008))

PREAMBLE

Timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents, is essential to the national security of the United States. All reasonable and lawful means must be used to ensure that the United States will receive the best intelligence possible. For that purpose, by virtue of the authority vested in me by the Constitution and the laws of the United States of America, including the National Security Act of 1947, as amended, (Act) and as President of the United States of America, in order to provide for the effective conduct of United States intelligence activities and the protection of constitutional rights, it is hereby ordered as follows:

PART 1 *Goals, Directions, Duties, and Responsibilities with Respect to United States Intelligence Efforts*

1.1 *Goals.* The United States intelligence effort shall provide the President, the National Security Council, and the Homeland Security Council with the necessary information on which to base decisions concerning the development and conduct of foreign, defense, and economic policies, and the protection of United States national interests from foreign security threats. All departments and agencies shall cooperate fully to fulfill this goal.

(a) All means, consistent with applicable Federal law and this order, and with full consideration of the rights of United States persons, shall be used to obtain reliable intelligence information to protect the United States and its interests.

(b) The United States Government has a solemn obligation, and shall continue in the conduct of intelligence activities under this order, to protect fully the legal rights of all United States persons, including freedoms, civil liberties, and privacy rights guaranteed by Federal law.

(c) Intelligence collection under this order should be guided by the need for information to respond to intelligence priorities set by the President.

(d) Special emphasis should be given to detecting and countering:

- (1) Espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests;
- (2) Threats to the United States and its interests from terrorism; and
- (3) Threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction.

(e) Special emphasis shall be given to the production of timely, accurate, and insightful reports, responsive to decisionmakers in the executive branch, that draw on all appropriate sources of information, including open source information, meet rigorous analytic standards, consider diverse analytic viewpoints, and accurately represent appropriate alternative views.

(f) State, local, and tribal governments are critical partners in securing and defending the United States from terrorism and other threats to the United States and its interests. Our national intelligence effort should take into account the responsibilities and requirements of State, local, and tribal governments and, as appropriate, private sector entities, when undertaking the collection and dissemination of information and intelligence to protect the United States.

(g) All departments and agencies have a responsibility to prepare and to provide intelligence in a manner that allows the full and free exchange of information, consistent with applicable law and presidential guidance.

1.2 *The National Security Council.*

(a) ***Purpose.*** The National Security Council (NSC) shall act as the highest ranking executive branch entity that provides support to the President for review of, guidance for, and direction to the conduct of all foreign intelligence, counterintelligence, and covert action, and attendant policies and programs.

(b) ***Covert Action and Other Sensitive Intelligence Operations.*** The NSC shall consider and submit to the President a policy recommendation, including all dissents, on each proposed covert action

and conduct a periodic review of ongoing covert action activities, including an evaluation of the effectiveness and consistency with current national policy of such activities and consistency with applicable legal requirements. The NSC shall perform such other functions related to covert action as the President may direct, but shall not undertake the conduct of covert actions. The NSC shall also review proposals for other sensitive intelligence operations.

1.3 Director of National Intelligence. Subject to the authority, direction, and control of the President, the Director of National Intelligence (Director) shall serve as the head of the Intelligence Community, act as the principal adviser to the President, to the NSC, and to the Homeland Security Council for intelligence matters related to national security, and shall oversee and direct the implementation of the National Intelligence Program and execution of the National Intelligence Program budget. The Director will lead a unified, coordinated, and effective intelligence effort. In addition, the Director shall, in carrying out the duties and responsibilities under this section, take into account the views of the heads of departments containing an element of the Intelligence Community and of the Director of the Central Intelligence Agency.

(a) Except as otherwise directed by the President or prohibited by law, the Director shall have access to all information and intelligence described in section 1.5(a) of this order. For the purpose of access to and sharing of information and intelligence, the Director:

(1) Is hereby assigned the function under section 3(5) of the Act, to determine that intelligence, regardless of the source from which derived and including information gathered within or outside the United States, pertains to more than one United States Government agency; and

(2) Shall develop guidelines for how information or intelligence is provided to or accessed by the Intelligence Community in accordance with section 1.5(a) of this order, and for how the information or intelligence may be used and shared by the Intelligence Community. All guidelines developed in accordance with this section shall be approved by the Attorney General and, where applicable, shall be consistent with guidelines issued pursuant to section 1016 of the Intelligence Reform and Terrorism Protection Act of 2004 (Public Law 108-458) (IRTPA).

(b) In addition to fulfilling the obligations and responsibilities prescribed by the Act, the Director:

(1) Shall establish objectives, priorities, and guidance for the Intelligence Community to ensure timely and effective collection, processing, analysis, and dissemination of intelligence, of whatever nature and from whatever source derived;

(2) May designate, in consultation with affected heads of departments or Intelligence Community elements, one or more Intelligence Community elements to develop and to maintain services of common concern on behalf of the Intelligence Community if the Director determines such services can be more efficiently or effectively accomplished in a consolidated manner;

(3) Shall oversee and provide advice to the President and the NSC with respect to all ongoing and proposed covert action programs;

(4) In regard to the establishment and conduct of intelligence arrangements and agreements with foreign governments and international organizations:

(A) May enter into intelligence and counterintelligence arrangements and agreements with foreign governments and international organizations;

(B) Shall formulate policies concerning intelligence and counterintelligence arrangements and agreements with foreign governments and international organizations; and

(C) Shall align and synchronize intelligence and counterintelligence foreign relationships among the elements of the Intelligence Community to further United States national security, policy, and intelligence objectives;

(5) Shall participate in the development of procedures approved by the Attorney General governing criminal drug intelligence activities abroad to ensure that these activities are consistent with foreign intelligence programs;

(6) Shall establish common security and access standards for managing and handling intelligence systems, information, and products, with special emphasis on facilitating:

(A) The fullest and most prompt access to and dissemination of information and intelligence practicable, assigning the highest priority to detecting, preventing,

preempting, and disrupting terrorist threats and activities against the United States, its interests, and allies; and

(B) The establishment of standards for an interoperable information sharing enterprise that facilitates the sharing of intelligence information among elements of the Intelligence Community;

(7) Shall ensure that appropriate departments and agencies have access to intelligence and receive the support needed to perform independent analysis;

(8) Shall protect, and ensure that programs are developed to protect, intelligence sources, methods, and activities from unauthorized disclosure;

(9) Shall, after consultation with the heads of affected departments and agencies, establish guidelines for Intelligence Community elements for:

(A) Classification and declassification of all intelligence and intelligence-related information classified under the authority of the Director or the authority of the head of a department or Intelligence Community element; and

(B) Access to and dissemination of all intelligence and intelligence-related information, both in its final form and in the form when initially gathered, to include intelligence originally classified by the head of a department or Intelligence Community element, except that access to and dissemination of information concerning United States persons shall be governed by procedures developed in accordance with Part 2 of this order;

(10) May, only with respect to Intelligence Community elements, and after consultation with the head of the originating Intelligence Community element or the head of the originating department, declassify, or direct the declassification of, information or intelligence relating to intelligence sources, methods, and activities. The Director may only delegate this authority to the Principal Deputy Director of National Intelligence;

(11) May establish, operate, and direct one or more national intelligence centers to address intelligence priorities;

(12) May establish Functional Managers and Mission Managers, and designate officers or employees of the United States to serve in these positions.

(A) Functional Managers shall report to the Director concerning the execution of their duties as Functional Managers, and may be charged with developing and implementing strategic guidance, policies, and procedures for activities related to a specific intelligence discipline or set of intelligence activities; set training and tradecraft standards; and ensure coordination within and across intelligence disciplines and Intelligence Community elements and with related nonintelligence activities. Functional Managers may also advise the Director on: the management of resources; policies and procedures; collection capabilities and gaps; processing and dissemination of intelligence; technical architectures; and other issues or activities determined by the Director.

(i) The Director of the National Security Agency is designated the Functional Manager for signals intelligence;

(ii) The Director of the Central Intelligence Agency is designated the Functional Manager for human intelligence; and

(iii) The Director of the National Geospatial-Intelligence Agency is designated the Functional Manager for geospatial intelligence.

(B) Mission Managers shall serve as principal substantive advisors on all or specified aspects of intelligence related to designated countries, regions, topics, or functional issues;

(13) Shall establish uniform criteria for the determination of relative priorities for the transmission of critical foreign intelligence, and advise the Secretary of Defense concerning the communications requirements of the Intelligence Community for the transmission of such communications;

(14) Shall have ultimate responsibility for production and dissemination of intelligence produced by the Intelligence Community and authority to levy analytic tasks on intelligence production organizations within the Intelligence Community, in consultation with the heads of the Intelligence Community elements concerned;

(15) May establish advisory groups for the purpose of obtaining advice from within the Intelligence Community to carry out the Director's responsibilities, to include Intelligence Community executive management committees composed of senior Intelligence Community leaders. Advisory groups shall consist of representatives from elements of the Intelligence Community, as designated by the Director, or other executive branch departments, agencies, and offices, as appropriate;

(16) Shall ensure the timely exploitation and dissemination of data gathered by national intelligence collection means, and ensure that the resulting intelligence is disseminated immediately to appropriate government elements, including military commands;

(17) Shall determine requirements and priorities for, and manage and direct the tasking, collection, analysis, production, and dissemination of, national intelligence by elements of the Intelligence Community, including approving requirements for collection and analysis and resolving conflicts in collection requirements and in the tasking of national collection assets of Intelligence Community elements (except when otherwise directed by the President or when the Secretary of Defense exercises collection tasking authority under plans and arrangements approved by the Secretary of Defense and the Director);

(18) May provide advisory tasking concerning collection and analysis of information or intelligence relevant to national intelligence or national security to departments, agencies, and establishments of the United States Government that are not elements of the Intelligence Community; and shall establish procedures, in consultation with affected heads of departments or agencies and subject to approval by the Attorney General, to implement this authority and to monitor or evaluate the responsiveness of United States Government departments, agencies, and other establishments;

(19) Shall fulfill the responsibilities in section 1.3(b)(17) and (18) of this order, consistent with applicable law and with full consideration of the rights of United States persons, whether information is to be collected inside or outside the United States;

(20) Shall ensure, through appropriate policies and procedures, the deconfliction, coordination, and integration of all intelligence activities conducted by an Intelligence Community element or funded by the National Intelligence Program. In accordance with these policies and procedures:

(A) The Director of the Federal Bureau of Investigation shall coordinate the clandestine collection of foreign intelligence collected through human sources or through human-enabled means and counterintelligence activities inside the United States;

(B) The Director of the Central Intelligence Agency shall coordinate the clandestine collection of foreign intelligence collected through human sources or through human-enabled means and counterintelligence activities outside the United States;

(C) All policies and procedures for the coordination of counterintelligence activities and the clandestine collection of foreign intelligence inside the United States shall be subject to the approval of the Attorney General; and

(D) All policies and procedures developed under this section shall be coordinated with the heads of affected departments and Intelligence Community elements;

(21) Shall, with the concurrence of the heads of affected departments and agencies, establish joint procedures to deconflict, coordinate, and synchronize intelligence activities conducted by an Intelligence Community element or funded by the National Intelligence Program, with intelligence activities, activities that involve foreign intelligence and security services, or activities that involve the use of clandestine methods, conducted by other United States Government departments, agencies, and establishments;

(22) Shall, in coordination with the heads of departments containing elements of the Intelligence Community, develop procedures to govern major system acquisitions funded in whole or in majority part by the National Intelligence Program;

(23) Shall seek advice from the Secretary of State to ensure that the foreign policy implications of proposed intelligence activities are considered, and shall ensure, through appropriate policies and procedures, that intelligence activities are conducted in a manner consistent with the responsibilities pursuant to law and presidential direction of Chiefs of United States Missions; and

(24) Shall facilitate the use of Intelligence Community products by the Congress in a secure manner.

(c) The Director's exercise of authorities in the Act and this order shall not abrogate the statutory or other responsibilities of the heads of departments of the United States Government or the Director of the Central Intelligence Agency. Directives issued and actions taken by the Director in the exercise of the Director's authorities and responsibilities to integrate, coordinate, and make the Intelligence Community more effective in providing intelligence related to national security shall be implemented by the elements of the Intelligence Community, provided that any department head whose department contains an element of the Intelligence Community and who believes that a directive or action of the Director violates the requirements of section 1018 of the IRTPA or this subsection shall bring the issue to the attention of the Director, the NSC, or the President for resolution in a manner that respects and does not abrogate the statutory responsibilities of the heads of the departments.

(d) Appointments to certain positions.

(1) The relevant department or bureau head shall provide recommendations and obtain the concurrence of the Director for the selection of: the Director of the National Security Agency, the Director of the National Reconnaissance Office, the Director of the National Geospatial-Intelligence Agency, the Under Secretary of Homeland Security for Intelligence and Analysis, the Assistant Secretary of State for Intelligence and Research, the Director of the Office of Intelligence and Counterintelligence of the Department of Energy, the Assistant Secretary for Intelligence and Analysis of the Department of the Treasury, and the Executive Assistant Director for the National Security Branch of the Federal Bureau of Investigation. If the Director does not concur in the recommendation, the department head may not fill the vacancy or make the recommendation to the President, as the case may be. If the department head and the Director do not reach an agreement on the selection or recommendation, the Director and the department head concerned may advise the President directly of the Director's intention to withhold concurrence.

(2) The relevant department head shall consult with the Director before appointing an individual to fill a vacancy or recommending to the President an individual be nominated to fill a vacancy in any of the following positions: the Under Secretary of Defense for Intelligence; the Director of the Defense Intelligence Agency; uniformed heads of the intelligence elements of the Army, the Navy, the Air Force, and the Marine Corps above the rank of Major General or Rear Admiral; the Assistant Commandant of the Coast Guard for Intelligence; and the Assistant Attorney General for National Security.

(e) Removal from certain positions.

(1) Except for the Director of the Central Intelligence Agency, whose removal the Director may recommend to the President, the Director and the relevant department head shall consult on the removal, or recommendation to the President for removal, as the case may be, of: the Director of the National Security Agency, the Director of the National Geospatial-Intelligence Agency, the Director of the Defense Intelligence Agency, the Under Secretary of Homeland Security for Intelligence and Analysis, the Assistant Secretary of State for Intelligence and Research, and the Assistant Secretary for Intelligence and Analysis of the Department of the Treasury. If the Director and the department head do not agree on removal, or recommendation for removal, either may make a recommendation to the President for the removal of the individual.

(2) The Director and the relevant department or bureau head shall consult on the removal of: the Executive Assistant Director for the National Security Branch of the Federal Bureau of Investigation, the Director of the Office of Intelligence and Counterintelligence of the Department of Energy, the Director of the National Reconnaissance Office, the Assistant Commandant of the Coast Guard for Intelligence, and the Under Secretary of Defense for Intelligence. With respect to an individual appointed by a department head, the department head may remove the individual upon the request of the Director; if the department head chooses not to remove the individual, either the Director or the department head may advise the President of the department head's intention to retain the individual. In the case of the Under Secretary of Defense for Intelligence,

the Secretary of Defense may recommend to the President either the removal or the retention of the individual. For uniformed heads of the intelligence elements of the Army, the Navy, the Air Force, and the Marine Corps, the Director may make a recommendation for removal to the Secretary of Defense.

(3) Nothing in this subsection shall be construed to limit or otherwise affect the authority of the President to nominate, appoint, assign, or terminate the appointment or assignment of any individual, with or without a consultation, recommendation, or concurrence.

1.4 The Intelligence Community. Consistent with applicable Federal law and with the other provisions of this order, and under the leadership of the Director, as specified in such law and this order, the Intelligence Community shall:

(a) Collect and provide information needed by the President and, in the performance of executive functions, the Vice President, the NSC, the Homeland Security Council, the Chairman of the Joint Chiefs of Staff, senior military commanders, and other executive branch officials and, as appropriate, the Congress of the United States;

(b) In accordance with priorities set by the President, collect information concerning, and conduct activities to protect against, international terrorism, proliferation of weapons of mass destruction, intelligence activities directed against the United States, international criminal drug activities, and other hostile activities directed against the United States by foreign powers, organizations, persons, and their agents;

(c) Analyze, produce, and disseminate intelligence;

(d) Conduct administrative, technical, and other support activities within the United States and abroad necessary for the performance of authorized activities, to include providing services of common concern for the Intelligence Community as designated by the Director in accordance with this order;

(e) Conduct research, development, and procurement of technical systems and devices relating to authorized functions and missions or the provision of services of common concern for the Intelligence Community;

(f) Protect the security of intelligence related activities, information, installations, property, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the Intelligence Community elements as are necessary;

(g) Take into account State, local, and tribal governments' and, as appropriate, private sector entities' information needs relating to national and homeland security;

(h) Deconflict, coordinate, and integrate all intelligence activities and other information gathering in accordance with section 1.3(b)(20) of this order; and

(i) Perform such other functions and duties related to intelligence activities as the President may direct.

1.5 Duties and Responsibilities of the Heads of Executive Branch Departments and Agencies. The heads of all departments and agencies shall:

(a) Provide the Director access to all information and intelligence relevant to the national security or that otherwise is required for the performance of the Director's duties, to include administrative and other appropriate management information, except such information excluded by law, by the President, or by the Attorney General acting under this order at the direction of the President;

(b) Provide all programmatic and budgetary information necessary to support the Director in developing the National Intelligence Program;

(c) Coordinate development and implementation of intelligence systems and architectures and, as appropriate, operational systems and architectures of their departments, agencies, and other elements with the Director to respond to national intelligence requirements and all applicable information sharing and security guidelines, information privacy, and other legal requirements;

(d) Provide, to the maximum extent permitted by law, subject to the availability of appropriations and not inconsistent with the mission of the department or agency, such further support to the Director as the Director may request, after consultation with the head of the department or agency, for the performance of the Director's functions;

(e) Respond to advisory tasking from the Director under section 1.3(b)(18) of this order to the greatest extent possible, in accordance with applicable policies established by the head of the responding department or agency;

(f) Ensure that all elements within the department or agency comply with the provisions of Part 2 of this order, regardless of Intelligence Community affiliation, when performing foreign intelligence and counterintelligence functions;

(g) Deconflict, coordinate, and integrate all intelligence activities in accordance with section 1.3(b)(20), and intelligence and other activities in accordance with section 1.3(b)(21) of this order;

(h) Inform the Attorney General, either directly or through the Federal Bureau of Investigation, and the Director of clandestine collection of foreign intelligence and counterintelligence activities inside the United States not coordinated with the Federal Bureau of Investigation;

(i) Pursuant to arrangements developed by the head of the department or agency and the Director of the Central Intelligence Agency and approved by the Director, inform the Director and the Director of the Central Intelligence Agency, either directly or through his designee serving outside the United States, as appropriate, of clandestine collection of foreign intelligence collected through human sources or through human-enabled means outside the United States that has not been coordinated with the Central Intelligence Agency; and

(j) Inform the Secretary of Defense, either directly or through his designee, as appropriate, of clandestine collection of foreign intelligence outside the United States in a region of combat or contingency military operations designated by the Secretary of Defense, for purposes of this paragraph, after consultation with the Director of National Intelligence.

1.6 Heads of Elements of the Intelligence Community. The heads of elements of the Intelligence Community shall:

(a) Provide the Director access to all information and intelligence relevant to the national security or that otherwise is required for the performance of the Director's duties, to include administrative and other appropriate management information, except such information excluded by law, by the President, or by the Attorney General acting under this order at the direction of the President;

(b) Report to the Attorney General possible violations of Federal criminal laws by employees and of specified Federal criminal laws by any other person as provided in procedures agreed upon by the Attorney General and the head of the department, agency, or establishment concerned, in a manner consistent with the protection of intelligence sources and methods, as specified in those procedures;

(c) Report to the Intelligence Oversight Board, consistent with Executive Order 13462 of February 29, 2008, and provide copies of all such reports to the Director, concerning any intelligence activities of their elements that they have reason to believe may be unlawful or contrary to executive order or presidential directive;

(d) Protect intelligence and intelligence sources, methods, and activities from unauthorized disclosure in accordance with guidance from the Director;

(e) Facilitate, as appropriate, the sharing of information or intelligence, as directed by law or the President, to State, local, tribal, and private sector entities;

(f) Disseminate information or intelligence to foreign governments and international organizations under intelligence or counterintelligence arrangements or agreements established in accordance with section 1.3(b)(4) of this order;

(g) Participate in the development of procedures approved by the Attorney General governing production and dissemination of information or intelligence resulting from criminal drug intelligence activities abroad if they have intelligence responsibilities for foreign or domestic criminal drug production and trafficking; and

(h) Ensure that the inspectors general, general counsels, and agency officials responsible for privacy or civil liberties protection for their respective organizations have access to any information or intelligence necessary to perform their official duties.

1.7 Intelligence Community Elements. Each element of the Intelligence Community shall have the duties and responsibilities specified below, in addition to those specified by law or elsewhere in this order. Intelligence Community elements within executive departments shall serve the information and intelligence needs of their respective heads of departments and also shall operate as part of an integrated Intelligence Community, as provided in law or this order.

(a) **THE CENTRAL INTELLIGENCE AGENCY.** The Director of the Central Intelligence Agency shall:

- (1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence;
- (2) Conduct counterintelligence activities without assuming or performing any internal security functions within the United States;
- (3) Conduct administrative and technical support activities within and outside the United States as necessary for cover and proprietary arrangements;
- (4) Conduct covert action activities approved by the President. No agency except the Central Intelligence Agency (or the Armed Forces of the United States in time of war declared by the Congress or during any period covered by a report from the President to the Congress consistent with the War Powers Resolution, Public Law 93-148) may conduct any covert action activity unless the President determines that another agency is more likely to achieve a particular objective;
- (5) Conduct foreign intelligence liaison relationships with intelligence or security services of foreign governments or international organizations consistent with section 1.3(b)(4) of this order;
- (6) Under the direction and guidance of the Director, and in accordance with section 1.3(b)(4) of this order, coordinate the implementation of intelligence and counterintelligence relationships between elements of the Intelligence Community and the intelligence or security services of foreign governments or international organizations; and
- (7) Perform such other functions and duties related to intelligence as the Director may direct.

(b) THE DEFENSE INTELLIGENCE AGENCY. The Director of the Defense Intelligence Agency shall:

- (1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence to support national and departmental missions;
- (2) Collect, analyze, produce, or, through tasking and coordination, provide defense and defense-related intelligence for the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, combatant commanders, other Defense components, and non-Defense agencies;
- (3) Conduct counterintelligence activities;
- (4) Conduct administrative and technical support activities within and outside the United States as necessary for cover and proprietary arrangements;
- (5) Conduct foreign defense intelligence liaison relationships and defense intelligence exchange programs with foreign defense establishments, intelligence or security services of foreign governments, and international organizations in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order;
- (6) Manage and coordinate all matters related to the Defense Attaché system; and
- (7) Provide foreign intelligence and counterintelligence staff support as directed by the Secretary of Defense.

(c) THE NATIONAL SECURITY AGENCY. The Director of the National Security Agency shall:

- (1) Collect (including through clandestine means), process, analyze, produce, and disseminate signals intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions;
- (2) Establish and operate an effective unified organization for signals intelligence activities, except for the delegation of operational control over certain operations that are conducted through other elements of the Intelligence Community. No other department or agency may engage in signals intelligence activities except pursuant to a delegation by the Secretary of Defense, after coordination with the Director;
- (3) Control signals intelligence collection and processing activities, including assignment of resources to an appropriate agent for such periods and tasks as required for the direct support of military commanders;
- (4) Conduct administrative and technical support activities within and outside the United States as necessary for cover arrangements;
- (5) Provide signals intelligence support for national and departmental requirements and for the conduct of military operations;

(6) Act as the National Manager for National Security Systems as established in law and policy, and in this capacity be responsible to the Secretary of Defense and to the Director;

(7) Prescribe, consistent with section 102A(g) of the Act, within its field of authorized operations, security regulations covering operating practices, including the transmission, handling, and distribution of signals intelligence and communications security material within and among the elements under control of the Director of the National Security Agency, and exercise the necessary supervisory control to ensure compliance with the regulations; and

(8) Conduct foreign cryptologic liaison relationships in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

(d) THE NATIONAL RECONNAISSANCE OFFICE. The Director of the National Reconnaissance Office shall:

(1) Be responsible for research and development, acquisition, launch, deployment, and operation of overhead systems and related data processing facilities to collect intelligence and information to support national and departmental missions and other United States Government needs; and

(2) Conduct foreign liaison relationships relating to the above missions, in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

(e) THE NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY. The Director of the National Geospatial-Intelligence Agency shall:

(1) Collect, process, analyze, produce, and disseminate geospatial intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions;

(2) Provide geospatial intelligence support for national and departmental requirements and for the conduct of military operations;

(3) Conduct administrative and technical support activities within and outside the United States as necessary for cover arrangements; and

(4) Conduct foreign geospatial intelligence liaison relationships, in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

(f) THE INTELLIGENCE AND COUNTERINTELLIGENCE ELEMENTS OF THE ARMY, NAVY, AIR FORCE, AND MARINE CORPS. The Commanders and heads of the intelligence and counterintelligence elements of the Army, Navy, Air Force, and Marine Corps shall:

(1) Collect (including through clandestine means), produce, analyze, and disseminate defense and defense-related intelligence and counterintelligence to support departmental requirements, and, as appropriate, national requirements;

(2) Conduct counterintelligence activities;

(3) Monitor the development, procurement, and management of tactical intelligence systems and equipment and conduct related research, development, and test and evaluation activities; and

(4) Conduct military intelligence liaison relationships and military intelligence exchange programs with selected cooperative foreign defense establishments and international organizations in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

(g) INTELLIGENCE ELEMENTS OF THE FEDERAL BUREAU OF INVESTIGATION. Under the supervision of the Attorney General and pursuant to such regulations as the Attorney General may establish, the intelligence elements of the Federal Bureau of Investigation shall:

(1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence to support national and departmental missions, in accordance with procedural guidelines approved by the Attorney General, after consultation with the Director;

(2) Conduct counterintelligence activities; and

(3) Conduct foreign intelligence and counterintelligence liaison relationships with intelligence, security, and law enforcement services of foreign governments or international organizations in accordance with sections 1.3(b)(4) and 1.7(a)(6) of this order.

(h) THE INTELLIGENCE AND COUNTERINTELLIGENCE ELEMENTS OF THE COAST GUARD. The Commandant of the Coast Guard shall:

(1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence including defense and defense-related information and intelligence to support national and departmental missions;

(2) Conduct counterintelligence activities;

(3) Monitor the development, procurement, and management of tactical intelligence systems and equipment and conduct related research, development, and test and evaluation activities; and

(4) Conduct foreign intelligence liaison relationships and intelligence exchange programs with foreign intelligence services, security services or international organizations in accordance with sections 1.3(b)(4), 1.7(a)(6), and, when operating as part of the Department of Defense, 1.10(i) of this order.

(i) THE BUREAU OF INTELLIGENCE AND RESEARCH, DEPARTMENT OF STATE; THE OFFICE OF INTELLIGENCE AND ANALYSIS, DEPARTMENT OF THE TREASURY; THE OFFICE OF NATIONAL SECURITY INTELLIGENCE, DRUG ENFORCEMENT ADMINISTRATION; THE OFFICE OF INTELLIGENCE AND ANALYSIS, DEPARTMENT OF HOMELAND SECURITY; AND THE OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE, DEPARTMENT OF ENERGY. The heads of the Bureau of Intelligence and Research, Department of State; the Office of Intelligence and Analysis, Department of the Treasury; the Office of National Security Intelligence, Drug Enforcement Administration; the Office of Intelligence and Analysis, Department of Homeland Security; and the Office of Intelligence and Counterintelligence, Department of Energy shall:

(1) Collect (overtly or through publicly available sources), analyze, produce, and disseminate information, intelligence, and counterintelligence to support national and departmental missions; and

(2) Conduct and participate in analytic or information exchanges with foreign partners and international organizations in accordance with sections 1.3(b)(4) and 1.7(a)(6) of this order.

(j) THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE. The Director shall collect (overtly or through publicly available sources), analyze, produce, and disseminate information, intelligence, and counterintelligence to support the missions of the Office of the Director of National Intelligence, including the National Counterterrorism Center, and to support other national missions.

1.8 The Department of State. In addition to the authorities exercised by the Bureau of Intelligence and Research under sections 1.4 and 1.7(i) of this order, the Secretary of State shall:

(a) Collect (overtly or through publicly available sources) information relevant to United States foreign policy and national security concerns;

(b) Disseminate, to the maximum extent possible, reports received from United States diplomatic and consular posts;

(c) Transmit reporting requirements and advisory taskings of the Intelligence Community to the Chiefs of United States Missions abroad; and

(d) Support Chiefs of United States Missions in discharging their responsibilities pursuant to law and presidential direction.

1.9 The Department of the Treasury. In addition to the authorities exercised by the Office of Intelligence and Analysis of the Department of the Treasury under sections 1.4 and 1.7(i) of this order the Secretary of the Treasury shall collect (overtly or through publicly available sources) foreign financial information and, in consultation with the Department of State, foreign economic information.

1.10 The Department of Defense. The Secretary of Defense shall:

(a) Collect (including through clandestine means), analyze, produce, and disseminate information and intelligence and be responsive to collection tasking and advisory tasking by the Director;

(b) Collect (including through clandestine means), analyze, produce, and disseminate defense and defense-related intelligence and counterintelligence, as required for execution of the Secretary's responsibilities;

(c) Conduct programs and missions necessary to fulfill national, departmental, and tactical intelligence requirements;

(d) Conduct counterintelligence activities in support of Department of Defense components and coordinate counterintelligence activities in accordance with section 1.3(b)(20) and (21) of this order;

(e) Act, in coordination with the Director, as the executive agent of the United States Government for signals intelligence activities;

(f) Provide for the timely transmission of critical intelligence, as defined by the Director, within the United States Government;

(g) Carry out or contract for research, development, and procurement of technical systems and devices relating to authorized intelligence functions;

(h) Protect the security of Department of Defense installations, activities, information, property, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the Department of Defense as are necessary;

(i) Establish and maintain defense intelligence relationships and defense intelligence exchange programs with selected cooperative foreign defense establishments, intelligence or security services of foreign governments, and international organizations, and ensure that such relationships and programs are in accordance with sections 1.3(b)(4), 1.3(b)(21) and 1.7(a)(6) of this order;

(j) Conduct such administrative and technical support activities within and outside the United States as are necessary to provide for cover and proprietary arrangements, to perform the functions described in sections (a) through (i) above, and to support the Intelligence Community elements of the Department of Defense; and

(k) Use the Intelligence Community elements within the Department of Defense identified in section 1.7(b) through (f) and, when the Coast Guard is operating as part of the Department of Defense, (h) above to carry out the Secretary of Defense's responsibilities assigned in this section or other departments, agencies, or offices within the Department of Defense, as appropriate, to conduct the intelligence missions and responsibilities assigned to the Secretary of Defense.

1.11 *The Department of Homeland Security.* In addition to the authorities exercised by the Office of Intelligence and Analysis of the Department of Homeland Security under sections 1.4 and 1.7(i) of this order, the Secretary of Homeland Security shall conduct, through the United States Secret Service, activities to determine the existence and capability of surveillance equipment being used against the President or the Vice President of the United States, the Executive Office of the President, and, as authorized by the Secretary of Homeland Security or the President, other Secret Service protectees and United States officials. No information shall be acquired intentionally through such activities except to protect against use of such surveillance equipment, and those activities shall be conducted pursuant to procedures agreed upon by the Secretary of Homeland Security and the Attorney General.

1.12 *The Department of Energy.* In addition to the authorities exercised by the Office of Intelligence and Counterintelligence of the Department of Energy under sections 1.4 and 1.7(i) of this order, the Secretary of Energy shall:

(a) Provide expert scientific, technical, analytic, and research capabilities to other agencies within the Intelligence Community, as appropriate;

(b) Participate in formulating intelligence collection and analysis requirements where the special expert capability of the Department can contribute; and

(c) Participate with the Department of State in overtly collecting information with respect to foreign energy matters.

1.13 *The Federal Bureau of Investigation.* In addition to the authorities exercised by the intelligence elements of the Federal Bureau of Investigation of the Department of Justice under sections 1.4 and 1.7(g) of this order and under the supervision of the Attorney General and pursuant to such regulations as the Attorney General may establish, the Director of the Federal Bureau of Investigation shall provide technical assistance, within or outside the United States, to foreign intelligence and law enforcement services, consistent with section 1.3(b)(20) and (21) of this order, as may be necessary to support national or departmental missions.

PART 2 *Conduct of Intelligence Activities*

2.1 *Need.* Timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents, is essential to informed

decisionmaking in the areas of national security, national defense, and foreign relations. Collection of such information is a priority objective and will be pursued in a vigorous, innovative, and responsible manner that is consistent with the Constitution and applicable law and respectful of the principles upon which the United States was founded.

2.2 Purpose. This Order is intended to enhance human and technical collection techniques, especially those undertaken abroad, and the acquisition of significant foreign intelligence, as well as the detection and countering of international terrorist activities, the spread of weapons of mass destruction, and espionage conducted by foreign powers. Set forth below are certain general principles that, in addition to and consistent with applicable laws, are intended to achieve the proper balance between the acquisition of essential information and protection of individual interests. Nothing in this Order shall be construed to apply to or interfere with any authorized civil or criminal law enforcement responsibility of any department or agency.

2.3 Collection of information. Elements of the Intelligence Community are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures established by the head of the Intelligence Community element concerned or by the head of a department containing such element and approved by the Attorney General, consistent with the authorities provided by Part 1 of this Order, after consultation with the Director. Those procedures shall permit collection, retention, and dissemination of the following types of information:

- (a) Information that is publicly available or collected with the consent of the person concerned;
- (b) Information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations. Collection within the United States of foreign intelligence not otherwise obtainable shall be undertaken by the Federal Bureau of Investigation (FBI) or, when significant foreign intelligence is sought, by other authorized elements of the Intelligence Community, provided that no foreign intelligence collection by such elements may be undertaken for the purpose of acquiring information concerning the domestic activities of United States persons;
- (c) Information obtained in the course of a lawful foreign intelligence, counterintelligence, international drug or international terrorism investigation;
- (d) Information needed to protect the safety of any persons or organizations, including those who are targets, victims, or hostages of international terrorist organizations;
- (e) Information needed to protect foreign intelligence or counterintelligence sources, methods, and activities from unauthorized disclosure. Collection within the United States shall be undertaken by the FBI except that other elements of the Intelligence Community may also collect such information concerning present or former employees, present or former intelligence element contractors or their present or former employees, or applicants for such employment or contracting;
- (f) Information concerning persons who are reasonably believed to be potential sources or contacts for the purpose of determining their suitability or credibility;
- (g) Information arising out of a lawful personnel, physical, or communications security investigation;
- (h) Information acquired by overhead reconnaissance not directed at specific United States persons;
- (i) Incidentally obtained information that may indicate involvement in activities that may violate Federal, state, local, or foreign laws; and
- (j) Information necessary for administrative purposes.

In addition, elements of the Intelligence Community may disseminate information to each appropriate element within the Intelligence Community for purposes of allowing the recipient element to determine whether the information is relevant to its responsibilities and can be retained by it, except that information derived from signals intelligence may only be disseminated or made available to Intelligence Community elements in accordance with procedures established by the Director in coordination with the Secretary of Defense and approved by the Attorney General.

2.4 Collection Techniques. Elements of the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad. Elements of the Intelligence Community are not authorized to use such techniques as electronic surveillance, unconsented physical searches, mail surveillance, physical surveillance, or monitoring devices unless

they are in accordance with procedures established by the head of the Intelligence Community element concerned or the head of a department containing such element and approved by the Attorney General, after consultation with the Director. Such procedures shall protect constitutional and other legal rights and limit use of such information to lawful governmental purposes. These procedures shall not authorize:

(a) The Central Intelligence Agency (CIA) to engage in electronic surveillance within the United States except for the purpose of training, testing, or conducting countermeasures to hostile electronic surveillance;

(b) Unconsented physical searches in the United States by elements of the Intelligence Community other than the FBI, except for:

(1) Searches by counterintelligence elements of the military services directed against military personnel within the United States or abroad for intelligence purposes, when authorized by a military commander empowered to approve physical searches for law enforcement purposes, based upon a finding of probable cause to believe that such persons are acting as agents of foreign powers; and

(2) Searches by CIA of personal property of non-United States persons lawfully in its possession;

(c) Physical surveillance of a United States person in the United States by elements of the Intelligence Community other than the FBI, except for:

(1) Physical surveillance of present or former employees, present or former intelligence element contractors or their present or former employees, or applicants for any such employment or contracting; and

(2) Physical surveillance of a military person employed by a non-intelligence element of a military service; and

(d) Physical surveillance of a United States person abroad to collect foreign intelligence, except to obtain significant information that cannot reasonably be acquired by other means.

2.5 Attorney General Approval. The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power. The authority delegated pursuant to this paragraph, including the authority to approve the use of electronic surveillance as defined in the Foreign Intelligence Surveillance Act of 1978, as amended, shall be exercised in accordance with that Act.

2.6 Assistance to Law Enforcement and other Civil Authorities. Elements of the Intelligence Community are authorized to:

(a) Cooperate with appropriate law enforcement agencies for the purpose of protecting the employees, information, property, and facilities of any element of the Intelligence Community;

(b) Unless otherwise precluded by law or this Order, participate in law enforcement activities to investigate or prevent clandestine intelligence activities by foreign powers, or international terrorist or narcotics activities;

(c) Provide specialized equipment, technical knowledge, or assistance of expert personnel for use by any department or agency, or when lives are endangered, to support local law enforcement agencies. Provision of assistance by expert personnel shall be approved in each case by the general counsel of the providing element or department; and

(d) Render any other assistance and cooperation to law enforcement or other civil authorities not precluded by applicable law.

2.7 Contracting. Elements of the Intelligence Community are authorized to enter into contracts or arrangements for the provision of goods or services with private companies or institutions in the United States and need not reveal the sponsorship of such contracts or arrangements for authorized intelligence purposes. Contracts or arrangements with academic institutions may be undertaken only with the consent of appropriate officials of the institution.

2.8 Consistency With Other Laws. Nothing in this Order shall be construed to authorize any activity in violation of the Constitution or statutes of the United States.

2.9 Undisclosed Participation in Organizations Within the United States. No one acting on behalf of elements of the Intelligence Community may join or otherwise participate in any organization in the United States on behalf of any element of the Intelligence Community without disclosing such person's intelligence affiliation to appropriate officials of the organization, except in accordance with procedures established by the head of the Intelligence Community element concerned or the head of a department containing such element and approved by the Attorney General, after consultation with the Director. Such participation shall be authorized only if it is essential to achieving lawful purposes as determined by the Intelligence Community element head or designee. No such participation may be undertaken for the purpose of influencing the activity of the organization or its members except in cases where:

- (a) The participation is undertaken on behalf of the FBI in the course of a lawful investigation; or
- (b) The organization concerned is composed primarily of individuals who are not United States persons and is reasonably believed to be acting on behalf of a foreign power.

2.10 Human Experimentation. No element of the Intelligence Community shall sponsor, contract for, or conduct research on human subjects except in accordance with guidelines issued by the Department of Health and Human Services. The subject's informed consent shall be documented as required by those guidelines.

2.11 Prohibition on Assassination. No person employed by or acting on behalf of the United States Government shall engage in or conspire to engage in assassination.

2.12 Indirect Participation. No element of the Intelligence Community shall participate in or request any person to undertake activities forbidden by this Order.

2.13 Limitation on Covert Action. No covert action may be conducted which is intended to influence United States political processes, public opinion, policies, or media.

PART 3 General Provisions

3.1 Congressional Oversight. The duties and responsibilities of the Director and the heads of other departments, agencies, elements, and entities engaged in intelligence activities to cooperate with the Congress in the conduct of its responsibilities for oversight of intelligence activities shall be implemented in accordance with applicable law, including title V of the Act. The requirements of applicable law, including title V of the Act, shall apply to all covert action activities as defined in this Order.

3.2 Implementation. The President, supported by the NSC, and the Director shall issue such appropriate directives, procedures, and guidance as are necessary to implement this order. Heads of elements within the Intelligence Community shall issue appropriate procedures and supplementary directives consistent with this order. No procedures to implement Part 2 of this order shall be issued without the Attorney General's approval, after consultation with the Director. The Attorney General shall provide a statement of reasons for not approving any procedures established by the head of an element in the Intelligence Community (or the head of the department containing such element) other than the FBI. In instances where the element head or department head and the Attorney General are unable to reach agreements on other than constitutional or other legal grounds, the Attorney General, the head of department concerned, or the Director shall refer the matter to the NSC.

3.3 Procedures. The activities herein authorized that require procedures shall be conducted in accordance with existing procedures or requirements established under Executive Order 12333. New procedures, as required by Executive Order 12333, as further amended, shall be established as expeditiously as possible. All new procedures promulgated pursuant to Executive Order 12333, as amended, shall be made available to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives.

3.4 *References and Transition.* References to "Senior Officials of the Intelligence Community" or "SOICs" in executive orders or other Presidential guidance, shall be deemed references to the heads of elements in the Intelligence Community, unless the President otherwise directs; references in Intelligence Community or Intelligence Community element policies or guidance, shall be deemed to be references to the heads of elements of the Intelligence Community, unless the President or the Director otherwise directs.

3.5 *Definitions.* For the purposes of this Order, the following terms shall have these meanings:

(a) *Counterintelligence* means information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.

(b) *Covert action* means an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly, but does not include:

(1) Activities the primary purpose of which is to acquire intelligence, traditional counterintelligence activities, traditional activities to improve or maintain the operational security of United States Government programs, or administrative activities;

(2) Traditional diplomatic or military activities or routine support to such activities;

(3) Traditional law enforcement activities conducted by United States Government law enforcement agencies or routine support to such activities; or

(4) Activities to provide routine support to the overt activities (other than activities described in paragraph (1), (2), or (3)) of other United States Government agencies abroad.

(c) *Electronic surveillance* means acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a nonelectronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter.

(d) *Employee* means a person employed by, assigned or detailed to, or acting for an element within the Intelligence Community.

(e) *Foreign intelligence* means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists.

(f) *Intelligence* includes foreign intelligence and counterintelligence.

(g) *Intelligence activities* means all activities that elements of the Intelligence Community are authorized to conduct pursuant to this order.

(h) *Intelligence Community* and elements of the Intelligence Community refers to:

(1) The Office of the Director of National Intelligence;

(2) The Central Intelligence Agency;

(3) The National Security Agency;

(4) The Defense Intelligence Agency;

(5) The National Geospatial-Intelligence Agency;

(6) The National Reconnaissance Office;

(7) The other offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs;

(8) The intelligence and counterintelligence elements of the Army, the Navy, the Air Force, and the Marine Corps;

(9) The intelligence elements of the Federal Bureau of Investigation;

(10) The Office of National Security Intelligence of the Drug Enforcement Administration;

(11) The Office of Intelligence and Counterintelligence of the Department of Energy;

(12) The Bureau of Intelligence and Research of the Department of State;

(13) The Office of Intelligence and Analysis of the Department of the Treasury;

(14) The Office of Intelligence and Analysis of the Department of Homeland Security;

(15) The intelligence and counterintelligence elements of the Coast Guard; and

(16) Such other elements of any department or agency as may be designated by the President, or designated jointly by the Director and the head of the department or agency concerned, as an element of the Intelligence Community.

(i) *National Intelligence and Intelligence Related to National Security* means all intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that pertains, as determined consistent with any guidance issued by the President, or that is determined for the purpose of access to information by the Director in accordance with section 1.3(a)(1) of this order, to pertain to more than one United States Government agency; and that involves threats to the United States, its people, property, or interests; the development, proliferation, or use of weapons of mass destruction; or any other matter bearing on United States national or homeland security.

(j) *The National Intelligence Program* means all programs, projects, and activities of the Intelligence Community, as well as any other programs of the Intelligence Community designated jointly by the Director and the head of a United States department or agency or by the President. Such term does not include programs, projects, or activities of the military departments to acquire intelligence solely for the planning and conduct of tactical military operations by United States Armed Forces.

(k) *United States person* means a United States citizen, an alien known by the intelligence element concerned to be a permanent resident alien, 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.

3.6 *Revocation.* Executive Orders 13354 and 13355 of August 27, 2004, are revoked; and paragraphs 1.3(b)(9) Executive Order 12958, as amended, are inconsistent with this Order.

3.7 *General Provisions.*

(a) Consistent with section 1.3(c) of this order, nothing in this order shall be construed to impair or otherwise affect:

(1) Authority granted by law to a department or agency, or the head thereof; or

(2) Functions of the Director of the Office of Management and Budget relating to budget, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies or entities, its officers, employees, or agents, or any other person.

Reference:

28 CFR Part 23

Executive Order 12291 These regulations are not a "major rule" as defined by section 1(b) of Executive Order No. 12291, 3 CFR part 127 (1981), because they do not result in: (a) An effect on the economy of \$100 million or more, (b) a major increase in any costs or prices, or (c) adverse effects on competition, employment, investment, productivity, or innovation among American enterprises.

Regulatory Flexibility Act

These regulations are not a rule within the meaning of the Regulatory Flexibility Act, 5 U.S.C. 601-612. These regulations, if promulgated, will not have a "significant" economic impact on a substantial number of small "entities," as defined by the Regulatory Flexibility Act.

Paperwork Reduction Act

There are no collection of information requirements contained in the proposed regulation.

List of Subjects in 28 CFR Part 23

Administrative practice and procedure, Grant programs, Intelligence, Law Enforcement.

For the reasons set out in the preamble, title 28, part 23 of the Code of Federal Regulations is revised to read as follows:

PART 23-CRIMINAL INTELLIGENCE SYSTEMS OPERATING POLICIES Sec.

23.1 Purpose.

23.2 Background.

23.3 Applicability.

23.20 Operating principles.

23.30 Funding guidelines.

23.40 Monitoring and auditing of grants for the funding of intelligence systems.

Authority: 42 U.S.C. 3782(a); 42 U.S.C. 3789g(c).

§ 23.1 Purpose.

The purpose of this regulation is to assure that all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, et seq., as amended (Pub. L. 90-351, as amended by Pub. L. 91-644, Pub. L. 93-83, Pub. L. 93-415, Pub. L. 94-430, Pub. L. 94-503, Pub. L. 95-115, Pub. L. 96-157, Pub. L. 98-473, Pub. L. 99-570, Pub. L. 100-690, and Pub. L. 101-647), are utilized in conformance with the privacy and constitutional rights of individuals.

§ 23.2 Background.

It is recognized that certain criminal activities including but not limited to loan sharking, drug trafficking, trafficking in stolen property, gambling, extortion, smuggling, bribery, and

corruption of public officials often involve some degree of regular coordination and permanent organization involving a large number of participants over a broad geographical area. The exposure of such ongoing networks of criminal activity can be aided by the pooling of information about such activities. However, because the collection and exchange of intelligence data necessary to support control of serious criminal activity may represent potential threats to the privacy of individuals to whom such data relates, policy guidelines for Federally funded projects are required.

§ 23.3 Applicability.

(a) These policy standards are applicable to all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, et seq., as amended (Pub. L. 90-351, as amended by Pub. L. 91-644, Pub. L. 93-83, Pub. L. 93-415, Pub. L. 94-430, Pub. L. 94-503, Pub. L. 95-115, Pub. L. 96-157, Pub. L. 98-473, Pub. L. 99-570, Pub. L. 100-690, and Pub. L. 101-647).

(b) As used in these policies: (1) Criminal Intelligence System or Intelligence System means the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information; (2)

Interjurisdictional Intelligence System

means an intelligence system which involves two or more participating agencies representing different governmental units or jurisdictions; (3) Criminal Intelligence Information means data which has been evaluated to determine that it: (i) is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity, and (ii) meets criminal intelligence system submission criteria; (4) Participating Agency means an agency of local, county, State, Federal, or other governmental unit which exercises law enforcement or criminal investigation authority and which is authorized to submit and receive criminal intelligence information through an interjurisdictional intelligence system. A participating agency may be a member or a nonmember of an interjurisdictional intelligence system; (5) Intelligence Project or Project means the organizational unit which operates an intelligence system on behalf of and for the benefit of a single agency or the organization which operates an interjurisdictional intelligence system on behalf of a group of participating agencies; and (6) Validation of Information means the procedures governing the periodic review of criminal intelligence information to assure its continuing compliance with system submission criteria established by regulation or program policy.

§ 23.20 Operating principles.

(a) A project shall collect and maintain criminal intelligence information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity.

(b) A project shall not collect or maintain criminal intelligence information about the political, religious or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless such information directly relates

to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity.

(c) Reasonable Suspicion or Criminal Predicate is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise. In an interjurisdictional intelligence system, the project is responsible for establishing the existence of reasonable suspicion of criminal activity either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.

(d) A project shall not include in any criminal intelligence system information which has been obtained in violation of any applicable Federal, State, or local law or ordinance. In an interjurisdictional intelligence system, the project is responsible for establishing that no information is entered in violation of Federal, State, or local laws, either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.

(e) A project or authorized recipient shall disseminate criminal intelligence information only where there is a need to know and a right to know the information in the performance of a law enforcement activity.

(f) (1) Except as noted in paragraph (f)(2) of this section, a project shall disseminate criminal intelligence information only to law enforcement authorities who shall agree to follow procedures regarding information receipt, maintenance, security, and dissemination which are consistent with these principles.

(2) Paragraph (f)(1) of this section shall not limit the dissemination of an assessment of criminal intelligence information to a government official or to any other individual, when necessary, to avoid imminent danger to life or property.

(g) A project maintaining criminal intelligence information shall ensure that administrative, technical, and physical safeguards (including audit trails) are adopted to insure against unauthorized access and against intentional or unintentional damage. A record indicating who has been given information, the reason for release of the information, and the date of each dissemination outside the project shall be kept. Information shall be labeled to indicate levels of sensitivity, levels of confidence, and the identity of submitting agencies and control officials. Each project must establish written definitions for the need to know and right to know standards for dissemination to other agencies as provided in paragraph (e) of this section. The project is responsible for establishing the existence of an inquirer's need to know and right to know the information being requested either through inquiry or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project. Each intelligence project shall assure that the following security requirements are implemented:

(1) Where appropriate, projects must adopt effective and technologically advanced computer software and hardware designs to prevent unauthorized access to the information contained in the system;

- (2) The project must restrict access to its facilities, operating environment and documentation to organizations and personnel authorized by the project;
 - (3) The project must store information in the system in a manner such that it cannot be modified, destroyed, accessed, or purged without authorization;
 - (4) The project must institute procedures to protect criminal intelligence information from unauthorized access, theft, sabotage, fire, flood, or other natural or manmade disaster;
 - (5) The project must promulgate rules and regulations based on good cause for implementing its authority to screen, reject for employment, transfer, or remove personnel authorized to have direct access to the system; and
 - (6) A project may authorize and utilize remote (off-premises) system data bases to the extent that they comply with these security requirements.
- (h) All projects shall adopt procedures to assure that all information which is retained by a project has relevancy and importance. Such procedures shall provide for the periodic review of information and the destruction of any information which is misleading, obsolete or otherwise unreliable and shall require that any recipient agencies be advised of such changes which involve errors or corrections. All information retained as a result of this review must reflect the name of the reviewer, date of review and explanation of decision to retain. Information retained in the system must be reviewed and validated for continuing compliance with system submission criteria before the expiration of its retention period, which in no event shall be longer than five (5) years.
- (i) If funds awarded under the Act are used to support the operation of an intelligence system, then:
- (1) No project shall make direct remote terminal access to intelligence information available to system participants, except as specifically approved by the Office of Justice Programs (OJP) based on a determination that the system has adequate policies and procedures in place to insure that it is accessible only to authorized systems users; and
 - (2) A project shall undertake no major modifications to system design without prior grantor agency approval.
- (j) A project shall notify the grantor agency prior to initiation of formal information exchange procedures with any Federal, State, regional, or other information systems not indicated in the grant documents as initially approved at time of award.
- (k) A project shall make assurances that there will be no purchase or use in the course of the project of any electronic, mechanical, or other device for surveillance purposes that is in violation of the provisions of the Electronic Communications Privacy Act of 1986, Public Law 99-508, 18 U.S.C. 2510-2520, 2701-2709 and 3121-3125, or any applicable State statute related to wiretapping and surveillance.
- (l) A project shall make assurances that there will be no harassment or interference with any lawful political activities as part of the intelligence operation.
- (m) A project shall adopt sanctions for unauthorized access, utilization, or disclosure of information contained in the system.
- (n) A participating agency of an interjurisdictional intelligence system must maintain in its agency files information which documents each submission to the system and supports

compliance with project entry criteria. Participating agency files supporting system submissions must be made available for reasonable audit and inspection by project representatives. Project representatives will conduct participating agency inspection and audit in such a manner so as to protect the confidentiality and sensitivity of participating agency intelligence records.

(o) The Attorney General or designee may waive, in whole or in part, the applicability of a particular requirement or requirements contained in this part with respect to a criminal intelligence system, or for a class of submitters or users of such system, upon a clear and convincing showing that such waiver would enhance the collection, maintenance or dissemination of information in the criminal intelligence system, while ensuring that such system would not be utilized in violation of the privacy and constitutional rights of individuals or any applicable state or federal law.

§ 23.30 Funding guidelines. The following funding guidelines shall apply to all Crime Control Act funded discretionary assistance awards and Bureau of Justice Assistance (BJA) formula grant program subgrants, a purpose of which is to support the operation of an intelligence system. Intelligence systems shall only be funded where a grantee/subgrantee agrees to adhere to the principles set forth above and the project meets the following criteria:

(a) The proposed collection and exchange of criminal intelligence information has been coordinated with and will support ongoing or proposed investigatory or prosecutorial activities relating to specific areas of criminal activity.

(b) The areas of criminal activity for which intelligence information is to be utilized represent a significant and recognized threat to the population and:

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

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

(3) Are not limited to one jurisdiction.

(c) The head of a government agency or an individual with general policy making authority who has been expressly delegated such control and supervision by the head of the agency will retain control and supervision of information collection and dissemination for the criminal intelligence system. This official shall certify in writing that he or she takes full responsibility and will be accountable for the information maintained by and disseminated from the system and that the operation of the system will be in compliance with the principles set forth in § 23.20.

(d) Where the system is an interjurisdictional criminal intelligence system, the governmental agency which exercises control and supervision over the operation of the system shall require that the head of that agency or an individual with general policymaking authority who has been expressly delegated such control and supervision by the head of the agency:

(1) assume official responsibility and accountability for actions taken in the name of the joint entity, and

(2) certify in writing that the official takes full responsibility and will be accountable for insuring that the information transmitted to the interjurisdictional system or to participating agencies will be in compliance with the principles set forth in § 23.20. The principles set forth in § 23.20 shall be made part of the by-laws or operating procedures for that system. Each participating agency,

as a condition of participation, must accept in writing those principles which govern the submission, maintenance and dissemination of information included as part of the interjurisdictional system. (e) Intelligence information will be collected, maintained and disseminated primarily for State and local law enforcement efforts, including efforts involving Federal participation.

§ 23.40 Monitoring and auditing of grants for the funding of intelligence systems.

(a) Awards for the funding of intelligence systems will receive specialized monitoring and audit in accordance with a plan designed to insure compliance with operating principles as set forth in § 23.20. The plan shall be approved prior to award of funds.

(b) All such awards shall be subject to a special condition requiring compliance with the principles set forth in § 23.20.

(c) An annual notice will be published by OJP which will indicate the existence and the objective of all systems for the continuing interjurisdictional exchange of criminal intelligence information which are subject to the 28 CFR Part 23 Criminal Intelligence Systems Policies.

Laurie Robinson
Acting Assistant Attorney General
Office of Justice Programs
(FR Doc. 93-22614 Filed 9-15-93; 8:45 am)

Criminal Intelligence Sharing Systems; Policy Clarification
[Federal Register: December 30, 1998 (Volume 63, Number 250)] [Page 71752-71753]
From the Federal Register Online via GPO Access [wais.access.gpo.gov]
DEPARTMENT OF JUSTICE 28 CFR Part 23
[OJP(BJA)-1177B]
RIN 1121-ZB40

REFERENCE:

1998 Policy Clarification on 28 CFR Part 23

AGENCY: Bureau of Justice Assistance (BJA), Office of Justice Programs (OJP), Justice.

ACTION: Clarification of policy.

SUMMARY: The current policy governing the entry of identifying information into criminal intelligence sharing systems requires clarification. This policy clarification is to make clear that the entry of individuals, entities and organizations, and locations that do not otherwise meet the requirements of reasonable suspicion is appropriate when it is done solely for the purposes of criminal identification or is germane to the criminal subject's criminal activity. Further, the definition of "criminal intelligence system" is clarified.

EFFECTIVE DATE: This clarification is effective December 30, 1998.

FOR FURTHER INFORMATION CONTACT: Paul Kendall, General Counsel, Office of Justice Programs, 810 7th Street NW, Washington, DC 20531, (202) 307-6235.

SUPPLEMENTARY INFORMATION: The operation of criminal intelligence information systems is governed by 28 CFR Part 23. This regulation was written to both protect the privacy rights of individuals and to encourage and expedite the exchange of criminal intelligence information between and among law enforcement agencies of different jurisdictions. Frequent interpretations of the regulation, in the form of policy guidance and correspondence, have been the primary method of ensuring that advances in technology did not hamper its effectiveness.

Comments:

The clarification was opened to public comment. Comments expressing unreserved support for the clarification were received from two Regional Intelligence Sharing Systems (RISS) and five states. A comment from the Chairperson of a RISS, relating to the use of identifying information to begin new investigations, has been incorporated. A single negative comment was received, but was not addressed to the subject of this clarification.

Use of Identifying Information:

28 CFR 23.3(b)(3) states that criminal intelligence information that can be put into a criminal intelligence sharing system is "information relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity, and . . . meets criminal intelligence system submission criteria."

Further, 28 CFR 23.20(a) states that a system shall only collect information on an individual if "there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity." 28 CFR 23.20(b) extends that limitation to [page 71753] collecting information on groups and corporate entities.

In an effort to protect individuals and organizations from the possible taint of having their names in intelligence systems (as defined at 28 CFR Sec. 23.3(b)(1)), the Office of Justice Programs has previously interpreted this section to allow information to be placed in a system only if that information independently meets the requirements of the regulation. Information that might be vital to identifying potential criminals, such as favored locations and companions, or names of family members, has been excluded from the systems. This policy has hampered the effectiveness of many criminal intelligence sharing systems.

Given the swiftly changing nature of modern technology and the expansion of the size and complexity of criminal organizations, the Bureau of Justice Assistance (BJA) has determined that it is necessary to clarify this element of 28 CFR Part 23. Many criminal intelligence databases are now employing "Comment" or "Modus Operandi" fields whose value would be greatly enhanced by the ability to store more detailed and wide-ranging identifying information. This may include names and limited data about people and organizations that are not suspected of any criminal activity or involvement, but merely aid in the identification and investigation of a criminal suspect who independently satisfies the reasonable suspicion standard.

Therefore, BJA issues the following clarification to the rules applying to the use of identifying information. Information that is relevant to the identification of a criminal suspect or to the criminal activity in which the suspect is engaged may be placed in a criminal intelligence database, provided that (1) appropriate disclaimers accompany the information noting that is strictly identifying information, carrying no criminal connotations; (2) identifying information may not be used as an independent basis to meet the requirement of reasonable suspicion of involvement in criminal activity necessary to create a record or file in a criminal intelligence system; and (3) the individual who is the criminal suspect identified by this information otherwise meets all requirements of 28 CFR Part 23. This information may be a searchable field in the intelligence system.

For example: A person reasonably suspected of being a drug dealer is known to conduct his criminal activities at the fictional "Northwest Market." An agency may wish to note this information in a criminal intelligence database, as it may be important to future identification of the suspect. Under the previous interpretation of the regulation, the entry of "Northwest Market" would not be permitted, because there was no reasonable suspicion that the "Northwest Market" was a criminal organization. Given the current clarification of the regulation, this will be permissible, provided that the information regarding the "Northwest Market" was clearly noted to be non-criminal in nature. For example, the data field in which "Northwest Market" was entered could be marked "Non-Criminal Identifying Information," or the words "Northwest Market" could be followed by a parenthetical comment such as "This organization has been entered into the system for identification purposes only - it is not suspected of any criminal activity or involvement." A criminal intelligence system record or file could not be created for "Northwest Market" solely on the basis of information provided, for example, in a comment field on the suspected drug dealer. Independent information would have to be obtained as a basis for the opening of a new criminal intelligence file or record based on reasonable suspicion on "Northwest Market." Further, the fact that other individuals frequent "Northwest Market" would not necessarily establish reasonable suspicion for those other individuals, as it relates to criminal intelligence systems.

The Definition of a "Criminal Intelligence System"

The definition of a "criminal intelligence system" is given in 28 CFR 23.3(b)(1) as the "arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information" Given the fact that cross-database searching techniques are now common-place, and given the fact that multiple databases may be contained on the same computer system, BJA has determined that this

definition needs clarification, specifically to differentiate between criminal intelligence systems and non-intelligence systems.

The comments to the 1993 revision of 28 CFR Part 23 noted that "the term 'intelligence system' is redefined to clarify the fact that historical telephone toll files, analytical information, and work products that are not either retained, stored, or exchanged and criminal history record information or identification (fingerprint) systems are excluded from the definition, and hence are not covered by the regulation" 58 FR 48448-48449 (Sept. 16, 1993.) The comments further noted that materials that "may assist an agency to produce investigative or other information for an intelligence system . . ." do not necessarily fall under the regulation. *Id.*

The above rationale for the exclusion of non-intelligence information sources from the definition of "criminal intelligence system," suggests now that, given the availability of more modern non-intelligence information sources such as the Internet, newspapers, motor vehicle administration records, and other public record information on-line, such sources shall not be considered part of criminal intelligence systems, and shall not be covered by this regulation, even if criminal intelligence systems access such sources during searches on criminal suspects. Therefore, criminal intelligence systems may conduct searches across the spectrum of non-intelligence systems without those systems being brought under 28 CFR Part 23. There is also no limitation on such non-intelligence information being stored on the same computer system as criminal intelligence information, provided that sufficient precautions are in place to separate the two types of information and to make it clear to operators and users of the information that two different types of information are being accessed.

Such precautions should be consistent with the above clarification of the rule governing the use of identifying information. This could be accomplished, for example, through the use of multiple windows, differing colors of data or clear labeling of the nature of information displayed.

Additional guidelines will be issued to provide details of the above clarifications as needed.

Dated: December 22, 1998.

Nancy Gist Director,
Bureau of Justice Assistance
[FR Doc. 98-34547 Filed 12-29-98; 8:45 am]
BILLING CODE 4410-18-P

Kansas Statute Annotated Chapter 45

45-220

**Chapter 45.--PUBLIC RECORDS, DOCUMENTS AND
INFORMATION Article 2.--RECORDS OPEN TO PUBLIC**

45-220. Procedures for obtaining access to or copies of records; request; office hours; provision of information on procedures. (a) Each public agency shall adopt procedures to be followed in requesting access to and obtaining copies of public records, which procedures shall provide full access to public records, protect public records from damage and disorganization, prevent excessive disruption of the agency's essential functions, provide assistance and information upon request and insure [ensure] efficient and timely action in response to applications for inspection of public records.

(b) A public agency may require a written request for inspection of public records but shall not otherwise require a request to be made in any particular form. Except as otherwise provided by subsection (c), a public agency shall not require that a request contain more information than the requester's name and address and the information necessary to ascertain the records to which the requester desires access and the requester's right of access to the records. A public agency may require proof of identity of any person requesting access to a public record. No request shall be returned, delayed or denied because of any technicality unless it is impossible to determine the records to which the requester desires access.

(c) If access to public records of an agency or the purpose for which the records may be used is limited pursuant to K.S.A. 45-221 or K.S.A. 2018 Supp. 45-230, and amendments thereto, the agency may require a person requesting the records or information therein to provide written certification that:

- (1) The requester has a right of access to the records and the basis of that right; or
- (2) the requester does not intend to, and will not: (A) Use any list of names or addresses contained in or derived from the records or information for the purpose of selling or offering for sale any property or service to any person listed or to any person who resides at any address listed; or (B) sell, give or otherwise make available to any person any list of names or addresses contained in or derived from the records or information for the purpose of allowing that person to sell or offer for sale any property or service to any person listed or to any person who resides at any address listed.

(d) A public agency shall establish, for business days when it does not maintain regular office hours, reasonable hours when persons may inspect and obtain copies of the agency's records. The public agency may require that any person desiring to inspect or obtain copies of the agency's records during such hours so notify the agency, but such notice shall not be required to be in writing and shall not be required to be given more than 24 hours prior to the hours established for inspection and obtaining copies.

(e) Each official custodian of public records shall designate such persons as necessary to carry out the duties of custodian under this act and shall ensure that a custodian is available during regular business hours of the public agency to carry out such duties.

(f) Each public agency shall provide, upon request of any person, the following information:

(1) The principal office of the agency, its regular office hours and any additional hours established by the agency pursuant to subsection (c).

(2) The title and address of the official custodian of the agency's records and of any other custodian who is ordinarily available to act on requests made at the location where the information is displayed.

(3) The fees, if any, charged for access to or copies of the agency's records.

(4) The procedures to be followed in requesting access to and obtaining copies of the agency's records, including procedures for giving notice of a desire to inspect or obtain copies of records during hours established by the agency pursuant to subsection (c).

(g) (1) Except for requests of summary data compiled from information submitted by multiple criminal justice agencies or as otherwise provided by law, requests for records submitted to the central repository or any other repositories supporting the criminal justice information system that are maintained by the Kansas bureau of investigation pursuant to K.S.A. 22-4704 and 22-4705, and amendments thereto, shall be directed to the criminal justice agency from which the records originated.

(2) As used in this subsection, the terms "central repository," "criminal justice agency" and "criminal justice information system" have the same meanings as defined in K.S.A. 22-4701, and amendments thereto.

(h) Except for requests of summary data compiled from information submitted by multiple law enforcement agencies or as otherwise provided by law, requests for records submitted to the Kansas asset seizure and forfeiture repository that are maintained by the Kansas bureau of investigation pursuant to K.S.A. 2018 Supp. 60-4127, and amendments thereto, shall be directed to the law enforcement agency from which the records originated.

(i) Requests for records defined as "files" pursuant to K.S.A. 2018 Supp. 75-4379, and amendments thereto, submitted to a state or local law enforcement agency or governmental agency shall be directed to the state or local law enforcement agency or governmental agency that made, maintained or kept such files, as required by K.S.A. 2018 Supp. 75-4379, and amendments thereto.

History: L. 1984, ch. 187, § 6; L. 1984, ch. 282, § 3; L. 2003, ch. 126, § 2; L. 2013, ch. 72, § 1; L. 2018, ch. 26, § 2; L. 2018, ch. 93, § 2; July 1.

45-221

Chapter 45.--PUBLIC RECORDS, DOCUMENTS AND INFORMATION Article 2.--RECORDS OPEN TO PUBLIC

45-221. Certain records not required to be open; separation of open and closed information required; statistics and records over 70 years old open. (a) Except to the extent disclosure is otherwise required by law, a public agency shall not be required to disclose:

(1) Records the disclosure of which is specifically prohibited or restricted by federal law, state statute or rule of the Kansas supreme court or rule of the senate committee on confirmation oversight relating to information submitted to the committee pursuant to K.S.A. 2018 Supp. 75-4315d, and amendments thereto, or the disclosure of which is prohibited or restricted pursuant to specific authorization of federal law, state statute or rule of the Kansas supreme court or rule of the senate committee on confirmation oversight relating to information submitted to the committee pursuant to K.S.A. 2018 Supp. 75-4315d, and amendments thereto, to restrict or prohibit disclosure.

(2) Records which are privileged under the rules of evidence, unless the holder of the privilege consents to the disclosure.

(3) Medical, psychiatric, psychological or alcoholism or drug dependency treatment records which pertain to identifiable patients.

(4) Personnel records, performance ratings or individually identifiable records pertaining to employees or applicants for employment, except that this exemption shall not apply to the names,

positions, salaries or actual compensation employment contracts or employment-related contracts or agreements and lengths of service of officers and employees of public agencies once they are employed as such.

(5) Information which would reveal the identity of any undercover agent or any informant reporting a specific violation of law.

(6) Letters of reference or recommendation pertaining to the character or qualifications of an identifiable individual, except documents relating to the appointment of persons to fill a vacancy in an elected office.

(7) Library, archive and museum materials contributed by private persons, to the extent of any limitations imposed as conditions of the contribution.

(8) Information which would reveal the identity of an individual who lawfully makes a donation to a public agency, if anonymity of the donor is a condition of the donation, except if the donation is intended for or restricted to providing remuneration or personal tangible benefit to a named public officer or employee.

(9) Testing and examination materials, before the test or examination is given or if it is to be given again, or records of individual test or examination scores, other than records which show only passage or failure and not specific scores.

(10) Criminal investigation records, except as provided herein. The district court, in an action brought pursuant to K.S.A. 45-222, and amendments thereto, may order disclosure of such records, subject to such conditions as the court may impose, if the court finds that disclosure:

(A) Is in the public interest;

(B) would not interfere with any prospective law enforcement action, criminal investigation or prosecution;

(C) would not reveal the identity of any confidential source or undercover agent;

(D) would not reveal confidential investigative techniques or procedures not known to the general public;

(E) would not endanger the life or physical safety of any person; and

(F) would not reveal the name, address, phone number or any other information which specifically and individually identifies the victim of any sexual offense in article 35 of chapter 21 of the Kansas Statutes Annotated, prior to their repeal, or article 55 of chapter 21 of the Kansas Statutes Annotated, and amendments thereto.

If a public record is discretionarily closed by a public agency pursuant to this subsection, the record custodian, upon request, shall provide a written citation to the specific provisions of paragraphs (A) through (F) that necessitate closure of that public record.

(11) Records of agencies involved in administrative adjudication or civil litigation, compiled in the process of detecting or investigating violations of civil law or administrative rules and regulations, if disclosure would interfere with a prospective administrative adjudication or civil litigation or reveal the identity of a confidential source or undercover agent.

(12) Records of emergency or security information or procedures of a public agency, or plans, drawings, specifications or related information for any building or facility which is used for purposes requiring security measures in or around the building or facility or which is used for the generation or transmission of power, water, fuels or communications, if disclosure would jeopardize security of the public agency, building or facility.

(13) The contents of appraisals or engineering or feasibility estimates or evaluations made by or for a public agency relative to the acquisition of property, prior to the award of formal contracts therefor.

(14) Correspondence between a public agency and a private individual, other than correspondence which is intended to give notice of an action, policy or determination relating to any regulatory, supervisory or enforcement responsibility of the public agency or which is widely

distributed to the public by a public agency and is not specifically in response to communications from such a private individual.

(15) Records pertaining to employer-employee negotiations, if disclosure would reveal information discussed in a lawful executive session under K.S.A. 75-4319, and amendments thereto.

(16) Software programs for electronic data processing and documentation thereof, but each public agency shall maintain a register, open to the public, that describes:

(A) The information which the agency maintains on computer facilities; and

(B) the form in which the information can be made available using existing computer programs.

(17) Applications, financial statements and other information submitted in connection with applications for student financial assistance where financial need is a consideration for the award.

(18) Plans, designs, drawings or specifications which are prepared by a person other than an employee of a public agency or records which are the property of a private person.

(19) Well samples, logs or surveys which the state corporation commission requires to be filed by persons who have drilled or caused to be drilled, or are drilling or causing to be drilled, holes for the purpose of discovery or production of oil or gas, to the extent that disclosure is limited by rules and regulations of the state corporation commission.

(20) Notes, preliminary drafts, research data in the process of analysis, unfunded grant proposals, memoranda, recommendations or other records in which opinions are expressed or policies or actions are proposed, except that this exemption shall not apply when such records are publicly cited or identified in an open meeting or in an agenda of an open meeting.

(21) Records of a public agency having legislative powers, which records pertain to proposed legislation or amendments to proposed legislation, except that this exemption shall not apply when such records are:

(A) Publicly cited or identified in an open meeting or in an agenda of an open meeting; or

(B) distributed to a majority of a quorum of any body which has authority to take action or make recommendations to the public agency with regard to the matters to which such records pertain.

(22) Records of a public agency having legislative powers, which records pertain to research prepared for one or more members of such agency, except that this exemption shall not apply when such records are:

(A) Publicly cited or identified in an open meeting or in an agenda of an open meeting; or

(B) distributed to a majority of a quorum of any body which has authority to take action or make recommendations to the public agency with regard to the matters to which such records pertain.

(23) Library patron and circulation records which pertain to identifiable individuals.

(24) Records which are compiled for census or research purposes and which pertain to identifiable individuals.

(25) Records which represent and constitute the work product of an attorney.

(26) Records of a utility or other public service pertaining to individually identifiable residential customers of the utility or service.

(27) Specifications for competitive bidding, until the specifications are officially approved by the public agency.

(28) Sealed bids and related documents, until a bid is accepted or all bids rejected.

(29) Correctional records pertaining to an identifiable inmate or release, except that:

(A) The name; photograph and other identifying information; sentence data; parole eligibility date; custody or supervision level; disciplinary record; supervision violations; conditions of supervision, excluding requirements pertaining to mental health or substance abuse

counseling; location of facility where incarcerated or location of parole office maintaining supervision and address of a releasee whose crime was committed after the effective date of this act shall be subject to disclosure to any person other than another inmate or releasee, except that the disclosure of the location of an inmate transferred to another state pursuant to the interstate corrections compact shall be at the discretion of the secretary of corrections;

(B) the attorney general, law enforcement agencies, counsel for the inmate to whom the record pertains and any county or district attorney shall have access to correctional records to the extent otherwise permitted by law;

(C) the information provided to the law enforcement agency pursuant to the sex offender registration act, K.S.A. 22-4901 et seq., and amendments thereto, shall be subject to disclosure to any person, except that the name, address, telephone number or any other information which specifically and individually identifies the victim of any offender required to register as provided by the Kansas offender registration act, K.S.A. 22-4901 et seq., and amendments thereto, shall not be disclosed; and

(D) records of the department of corrections regarding the financial assets of an offender in the custody of the secretary of corrections shall be subject to disclosure to the victim, or such victim's family, of the crime for which the inmate is in custody as set forth in an order of restitution by the sentencing court.

(30) Public records containing information of a personal nature where the public disclosure thereof would constitute a clearly unwarranted invasion of personal privacy.

(31) Public records pertaining to prospective location of a business or industry where no previous public disclosure has been made of the business' or industry's interest in locating in, relocating within or expanding within the state. This exception shall not include those records pertaining to application of agencies for permits or licenses necessary to do business or to expand business operations within this state, except as otherwise provided by law.

(32) Engineering and architectural estimates made by or for any public agency relative to public improvements.

(33) Financial information submitted by contractors in qualification statements to any public agency.

(34) Records involved in the obtaining and processing of intellectual property rights that are expected to be, wholly or partially vested in or owned by a state educational institution, as defined in K.S.A. 76-711, and amendments thereto, or an assignee of the institution organized and existing for the benefit of the institution.

(35) Any report or record which is made pursuant to K.S.A. 65-4922, 65-4923 or 65-4924, and amendments thereto, and which is privileged pursuant to K.S.A. 65-4915 or 65-4925, and amendments thereto.

(36) Information which would reveal the precise location of an archeological site.

(37) Any financial data or traffic information from a railroad company, to a public agency, concerning the sale, lease or rehabilitation of the railroad's property in Kansas.

(38) Risk-based capital reports, risk-based capital plans and corrective orders including the working papers and the results of any analysis filed with the commissioner of insurance in accordance with K.S.A. 40-2c20 and 40-2d20, and amendments thereto.

(39) Memoranda and related materials required to be used to support the annual actuarial opinions submitted pursuant to K.S.A. 40-409(b), and amendments thereto.

(40) Disclosure reports filed with the commissioner of insurance under K.S.A. 40-2,156(a), and amendments thereto.

(41) All financial analysis ratios and examination synopses concerning insurance companies that are submitted to the commissioner by the national association of insurance commissioners' insurance regulatory information system.

(42) Any records the disclosure of which is restricted or prohibited by a tribal-state gaming compact.

(43) Market research, market plans, business plans and the terms and conditions of managed care or other third-party contracts, developed or entered into by the university of Kansas medical center in the operation and management of the university hospital which the chancellor of the university of Kansas or the chancellor's designee determines would give an unfair advantage to competitors of the university of Kansas medical center.

(44) The amount of franchise tax paid to the secretary of revenue or the secretary of state by domestic corporations, foreign corporations, domestic limited liability companies, foreign limited liability companies, domestic limited partnership, foreign limited partnership, domestic limited liability partnerships and foreign limited liability partnerships.

(45) Records, other than criminal investigation records, the disclosure of which would pose a substantial likelihood of revealing security measures that protect: (A) Systems, facilities or equipment used in the production, transmission or distribution of energy, water or communications services; (B) transportation and sewer or wastewater treatment systems, facilities or equipment; or (C) private property or persons, if the records are submitted to the agency. For purposes of this paragraph, security means measures that protect against criminal acts intended to intimidate or coerce the civilian population, influence government policy by intimidation or coercion or to affect the operation of government by disruption of public services, mass destruction, assassination or kidnapping. Security measures include, but are not limited to, intelligence information, tactical plans, resource deployment and vulnerability assessments.

(46) Any information or material received by the register of deeds of a county from military discharge papers, DD Form 214. Such papers shall be disclosed: To the military dischargee; to such dischargee's immediate family members and lineal descendants; to such dischargee's heirs, agents or assigns; to the licensed funeral director who has custody of the body of the deceased dischargee; when required by a department or agency of the federal or state government or a political subdivision thereof; when the form is required to perfect the claim of military service or honorable discharge or a claim of a dependent of the dischargee; and upon the written approval of the commissioner of veterans affairs, to a person conducting research.

(47) Information that would reveal the location of a shelter or a safehouse or similar place where persons are provided protection from abuse or the name, address, location or other contact information of alleged victims of stalking, domestic violence or sexual assault.

(48) Policy information provided by an insurance carrier in accordance with K.S.A. 44-532(h)(1), and amendments thereto. This exemption shall not be construed to preclude access to an individual employer's record for the purpose of verification of insurance coverage or to the department of labor for their business purposes.

(49) An individual's e-mail address, cell phone number and other contact information which has been given to the public agency for the purpose of public agency notifications or communications which are widely distributed to the public.

(50) Information provided by providers to the local collection point administrator or to the 911 coordinating council pursuant to the Kansas 911 act, and amendments thereto, upon request of the party submitting such records.

(51) Records of a public agency on a public website which are searchable by a keyword search and identify the home address or home ownership of a law enforcement officer as defined in K.S.A. 2018 Supp. 21-5111, and amendments thereto, parole officer, probation officer, court services officer or community correctional services officer. Such individual officer shall file with the custodian of such record a request to have such officer's identifying information restricted from public access on such public website. Within 10 business days of receipt of such requests, the public agency shall restrict such officer's identifying information from such public access.

Such restriction shall expire after five years and such officer may file with the custodian of such record a new request for restriction at any time.

(52) Records of a public agency on a public website which are searchable by a keyword search and identify the home address or home ownership of a federal judge, a justice of the supreme court, a judge of the court of appeals, a district judge, a district magistrate judge, a municipal judge, the United States attorney for the district of Kansas, an assistant United States attorney, a special assistant United States attorney, the attorney general, an assistant attorney general, a special assistant attorney general, a county attorney, an assistant county attorney, a special assistant county attorney, a district attorney, an assistant district attorney, a special assistant district attorney, a city attorney, an assistant city attorney or a special assistant city attorney. Such person shall file with the custodian of such record a request to have such person's identifying information restricted from public access on such public website. Within 10 business days of receipt of such requests, the public agency shall restrict such person's identifying information from such public access. Such restriction shall expire after five years and such person may file with the custodian of such record a new request for restriction at any time.

(53) Records of a public agency that would disclose the name, home address, zip code, e-mail address, phone number or cell phone number or other contact information for any person licensed to carry concealed handguns or of any person who enrolled in or completed any weapons training in order to be licensed or has made application for such license under the personal and family protection act, K.S.A. 2018 Supp. 75-7c01 et seq., and amendments thereto, shall not be disclosed unless otherwise required by law.

(54) Records of a utility concerning information about cyber security threats, attacks or general attempts to attack utility operations provided to law enforcement agencies, the state corporation commission, the federal energy regulatory commission, the department of energy, the southwest power pool, the North American electric reliability corporation, the federal communications commission or any other federal, state or regional organization that has a responsibility for the safeguarding of telecommunications, electric, potable water, waste water disposal or treatment, motor fuel or natural gas energy supply systems.

(55) Records of a public agency containing information or reports obtained and prepared by the office of the state bank commissioner in the course of licensing or examining a person engaged in money transmission business pursuant to K.S.A. 9-508 et seq., and amendments thereto, shall not be disclosed except pursuant to K.S.A. 9-513c, and amendments thereto, or unless otherwise required by law.

(b) Except to the extent disclosure is otherwise required by law or as appropriate during the course of an administrative proceeding or on appeal from agency action, a public agency or officer shall not disclose financial information of a taxpayer which may be required or requested by a county appraiser or the director of property valuation to assist in the determination of the value of the taxpayer's property for ad valorem taxation purposes; or any financial information of a personal nature required or requested by a public agency or officer, including a name, job description or title revealing the salary or other compensation of officers, employees or applicants for employment with a firm, corporation or agency, except a public agency. Nothing contained herein shall be construed to prohibit the publication of statistics, so classified as to prevent identification of particular reports or returns and the items thereof.

(c) As used in this section, the term "cited or identified" shall not include a request to an employee of a public agency that a document be prepared.

(d) If a public record contains material which is not subject to disclosure pursuant to this act, the public agency shall separate or delete such material and make available to the requester that material in the public record which is subject to disclosure pursuant to this act. If a public record is not subject to disclosure because it pertains to an identifiable individual, the public agency

shall delete the identifying portions of the record and make available to the requester any remaining portions which are subject to disclosure pursuant to this act, unless the request is for a record pertaining to a specific individual or to such a limited group of individuals that the individuals' identities are reasonably ascertainable, the public agency shall not be required to disclose those portions of the record which pertain to such individual or individuals.

(e) The provisions of this section shall not be construed to exempt from public disclosure statistical information not descriptive of any identifiable person.

(f) Notwithstanding the provisions of subsection (a), any public record which has been in existence more than 70 years shall be open for inspection by any person unless disclosure of the record is specifically prohibited or restricted by federal law, state statute or rule of the Kansas supreme court or by a policy adopted pursuant to K.S.A. 72-6214, and amendments thereto.

(g) Any confidential records or information relating to security measures provided or received under the provisions of subsection (a)(45) shall not be subject to subpoena, discovery or other demand in any administrative, criminal or civil action.

History: L. 1984, ch. 187, § 7; L. 1984, ch. 282, § 4; L. 1986, ch. 193, § 1; L. 1987, ch. 176, § 4; L. 1989, ch. 154, § 1; L. 1991, ch. 149, § 12; L. 1994, ch. 107, § 8; L. 1995, ch. 44, § 1; L. 1995, ch. 257, § 6; L. 1996, ch. 256, § 15; L. 1997, ch. 126, § 44; L. 1997, ch. 181, § 15; L. 2000, ch. 156, § 3; L. 2001, ch. 211, § 13; L. 2002, ch. 178, § 1; L. 2003, ch. 109, § 22; L. 2004, ch. 171, § 30; L. 2005, ch. 126, § 1; L. 2008, ch. 121, § 4; L. 2009, ch. 83, § 27; L. 2009, ch. 125, § 1; L. 2010, ch. 112, § 2; L. 2011, ch. 30, § 192; L. 2011, ch. 84, § 23; L. 2012, ch. 147, § 1; L. 2013, ch. 72, § 2; L. 2013, ch. 133, § 18; L. 2014, ch. 120, § 6; L. 2015, ch. 68, § 10; July 1.