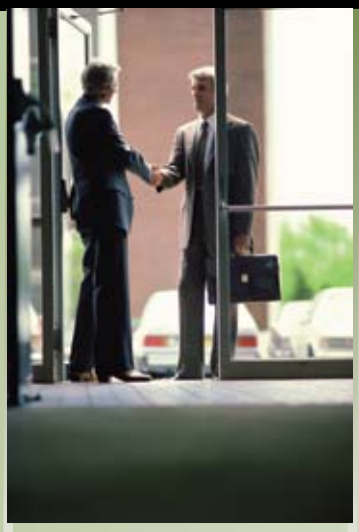
Global Justice Information Sharing Initiative

United States Department of Justice

DHS/DOJ Fusion Process Technical Assistance Program and Services

Fusion Center Privacy Policy Development



Privacy, Civil Rights, and Civil Liberties Policy Template

Revised With U.S. Department of Homeland Security Grant Program Guidance Requirements

April 2010

DHS/DOJ Fusion Process Technical Assistance Program and Services

Fusion Center Privacy Policy Development

Privacy, Civil Rights, and Civil Liberties Policy Template

April 2010

To request a Word version of this template, please submit your request to GLOBAL@iir.com.

About Global

The U.S. Department of Justice's Global Justice Information Sharing Initiative (Global) serves as a Federal Advisory Committee to the U.S. Attorney General on critical justice information sharing initiatives. Global promotes standards-based electronic information exchange to provide justice and public safety communities with timely, accurate, complete, and accessible information in a secure and trusted environment. Global is administered by the U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance.

This project was supported by Grant No. 2008-DD-BX-K520 awarded by the Bureau of Justice Assistance, Office of Justice Programs, in collaboration with the U.S. Department of Justice's Global Justice Information Sharing Initiative and the U.S. Department of Homeland Security. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the U.S. Department of Justice or the U.S. Department of Homeland Security.

Contents

Introduction **1**

I. What Is a Privacy, Civil Rights, and Civil Liberties Policy? 1
II. Benefits of a Privacy Policy 1
III. Template Purpose 2
IV. How to Use This Template 2
V. Template Modifications—Customizing Your Policy 2
VI. The Information Sharing Environment (ISE) 3
VII. The ISE and Fusion Centers 3
VIII. Resource List 3

Policy Development Template **5**

A. Purpose Statement 5
B. Policy Applicability and Legal Compliance 7
C. Governance and Oversight 9
D. Definitions 10
E. Information 11
F. Acquiring and Receiving Information 17
G. Information Quality Assurance 19
H. Collation and Analysis 21
I. Merging Records 22
J. Sharing and Disclosure 23
K. Redress… 27
K.1 Disclosure 27
K.2 Corrections 28
K.3 Appeals 28
K.4 Complaints 28
L. Security Safeguards 30

M. Information Retention and Destruction 32
N. Accountability and Enforcement 34
N.1 Information System Transparency 34
N.2 Accountability 34
N.3 Enforcement 36
O. Training… 37

Appendix A—Terms and Definitions 39

Appendix B—Federal Laws Relevant to Seeking, Retaining, and Disseminating Justice Information 47

Appendix C—Suspicious Activity Reporting (SAR) Summary of Provisions 49

Introduction

An intelligence fusion center is an effective and efficient mechanism to exchange information and intelligence, maximize resources, streamline operations, and improve the ability to fight crime and terrorism by analyzing data from a variety of sources. Today's increased security needs not only dictate enhanced information sharing but also highlight the need to balance the sharing of information with the rights of citizens. Ethical and legal obligations compel personnel, authorized users, and participating entities to protect constitutional rights, including privacy and other civil liberties, and civil rights throughout the information sharing process. To accomplish this, appropriate privacy and civil liberties protection policies must be in place.

I. What Is a Privacy, Civil Rights, and Civil Liberties Policy?

A privacy, civil rights, and civil liberties policy (privacy policy) is a written, published statement that articulates the center's position on how it handles the personally identifiable information and other personal, sensitive information it seeks or receives and uses in the normal course of business (see the definition of "personally identifiable information" in Appendix A, Terms and Definitions). The purpose of a privacy policy is to articulate within the center, to external agencies that access and share information with the center, to other entities, and publicly that the center will adhere to legal requirements and center policy and procedural provisions that enable gathering and sharing of information to occur in a manner that protects constitutional rights, including personal privacy and other civil liberties, and civil rights.

Privacy protections should be formulated in the planning and development stages of a justice information sharing system and must be fully implemented. As systems are designed, a privacy impact analysis or assessment should be conducted and protections should be developed for personally identifiable information and other personal, sensitive information to ensure that it is not improperly collected or distributed (see http://www.ojp.usdoj.gov/BJA/pdf/PIAGuide-Feb09.pdf). A privacy policy is different from a security policy. Although security policies protect certain aspects of privacy, their main function is to protect organizational assets and the organization's reputation. They do not focus on protecting individuals from harm, consider whether personal information should be gathered or collected in the first place, address data quality, specify how information and intelligence should be used or stored and with whom it should be shared, or establish policy on retention. A comprehensive privacy policy will address both security and privacy, including key privacy, civil rights, and civil liberties protection issues.

II. Benefits of a Privacy Policy

A strong privacy policy is good public policy, because it is responsive to widely held public expectations about the collection and use of information about individuals and the fair and open operation of a democratic government. A well-developed privacy policy protects the center,

external agencies that access and share information with the center, and their employees from liability under lawsuits and civil rights and civil liberties complaints; protects the public fisc; and promotes public trust in information sharing. A comprehensive policy that is properly enforced will also result in more effective and efficient use of public resources.

III. Template Purpose

Existing federal and state constitutional provisions, statutes, rules, and regulations forbid certain conduct and prescribe what and how information can be collected, used, maintained (including storage, review, and validation/purge), and shared. However, there may be gaps in these provisions—areas in which centers and individuals can exercise discretion in deciding how to proceed. Centers are encouraged to adopt policies and practices based on the exercise of this discretion in a manner that leads to more comprehensive protection of privacy, civil rights, and civil liberties. This workbook is provided to assist center personnel in developing a privacy policy related to the information the center collects, receives, maintains, archives, accesses, and discloses to center personnel, governmental agencies,

To assist centers that have completed a draft policy but need to add Information Sharing Environment (ISE) or suspicious activity reporting (SAR) provisions, sections containing ISE components are boxed and sections containing SAR components are shaded.

Information Sharing Environment (ISE) participants, and other participating criminal justice and public safety agencies, as well as to private contractors and the general public. The provisions suggested in this template are intended to be incorporated into the center's general operational policies and day-to-day operations and to provide explicit and detailed privacy protection guidance to center personnel and other authorized source and user agencies. Each section is a fundamental component of a comprehensive policy that includes baseline provisions on information collection, information quality, collation and analysis, merging records, information access and disclosure, redress, security safeguards, retention and destruction, accountability and enforcement, and training.

IV. How to Use This Template

This template is designed with privacy policy concepts grouped into related sections. Each section contains pertinent questions in the left-hand column and useful policy sample language in the right-hand column. To assist centers that have completed a draft policy but need to add Information Sharing Environment (ISE) or suspicious activity reporting (SAR) provisions, sections containing ISE components are boxed and sections containing SAR components are shaded. Also, a summary of SAR provisions is provided in Appendix C, Suspicious Activity Reporting (SAR) Summary of

Each section contains pertinent questions in the left-hand column and useful policy sample language in the right-hand column.

Provisions. For more information on the ISE, refer to Section VI., The Information Sharing Environment, and Section VII., The ISE and Fusion Centers.

Frequently, fusion centers have existing privacy-related policies and practices described in broader policy documents (e.g., concept of operations, standard operating procedures, and employee handbooks). In accordance with template Sections N, Accountability and Enforcement, and N.1, Information System Transparency, agencies are strongly encouraged to make their privacy policies available to the public, even if the other existing policies are not made available publicly. As such, consolidating existing policies into one privacy policy is highly recommended. Centers are cautioned, however, against simply providing a cross-reference to other policies in effect. Cross-referencing, without the applicable policy language, should be done only if those policies are also available to the public; otherwise, centers should restate the applicable language in their privacy policies.

V. Template Modifications—Customizing Your Policy

It is important to note that this privacy policy template is not intended to be used **as is,** without modification. Each section represents the foundational components

of an effective privacy policy but does not cover all concepts particular to your center, its unique processes and procedures, or the specific constitutional provisions, laws, ordinances, or regulations applicable within your state. Further, certain concepts or questions may not be applicable. The template represents a starting point for your center to establish minimum baseline privacy protections. Centers are encouraged to complete as many of the template questions as are applicable and to enhance sections to include items such as references to applicable statutes, rules, standards, or policies and to provide additional sections for provisions that are not addressed.

VI. The Information Sharing Environment (ISE)

In accordance with Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended, the ISE is a conceptual framework composed of the policies, procedures, and technologies linking the resources (people, systems, databases, and information) of state, local, and tribal (SLT) agencies; federal agencies; and the private sector to facilitate terrorism-related information sharing, access, and collaboration. Consistent with Presidential Guideline 5, the U.S. Attorney General, the U.S. Department of Justice (DOJ), and the Director of National Intelligence (DNI)—in coordination with the Program Manager for the ISE (PM-ISE) and the heads of federal departments and agencies that possess or use intelligence or other terrorism-related information—developed privacy guidelines for the ISE, titled *Guidelines to Ensure That the Information Privacy and Other Legal Rights of Americans Are Protected in the Development and Use of the Information Sharing Environment* (ISE Privacy Guidelines). The ISE Privacy Guidelines describe the means by which federal departments and agencies participating in the ISE will protect privacy and civil liberties in the development and operation of the ISE.

VII. The ISE and Fusion Centers

According to the ISE Privacy Guidelines, "Protected information [see Appendix A, Terms and Definitions] should be shared through the ISE only if it is terrorism information, homeland security information, or law enforcement information related to terrorism (terrorism-related information)." Fusion centers serve as the primary points of contact within states or regions for further dissemination of terrorism-related information consistent with DOJ's *Fusion Center Guidelines* and applicable SLT laws and regulations. As the ISE develops, fusion centers and possibly other SLT agencies receiving or sharing terrorism-related information will be required to parallel the ISE Privacy Guidelines in their privacy policies to be eligible to access and use federal agency terrorism-related information. The ISE Privacy Guidelines state "that such nonfederal entities develop and implement appropriate policies and procedures that provide protections (for terrorism-related information) that are **at least as comprehensive** as those contained in these Guidelines." To facilitate centers in meeting this requirement, this privacy policy template has incorporated the primary components of the ISE Privacy Guidelines. Throughout the template, sections expressly referencing ISE components are boxed for emphasis. These enhanced protections for terrorism-related information are neither required for the collection and sharing of other types of information and intelligence nor do they, in any manner, restrict fusion centers from collecting and sharing "all crimes–all hazards" information.

VIII. Resource List

This template incorporates the guidelines and requirements contained within the following documents and online resources:

- U.S. Department of Justice's (DOJ's) *Privacy and Civil Liberties Policy Development Guide and Implementation Templates*, Global Justice Information Sharing Initiative's (Global) Privacy and Information Quality Working Group, http://it.ojp.gov/documents/Privacy_Guide_Final.pdf
- DOJ's *Privacy, Civil Rights, and Civil Liberties Policy Templates for Justice Information Systems*, Global Privacy and Information Quality Working Group and the Justice Management Institute, http://it.ojp.gov/documents/Privacy_Civil_Rights_and_Civil_Liberties_Policy_Templates.pdf
- DOJ's *Fusion Center Guidelines: Law Enforcement Intelligence, Public Safety, and the Private Sector*, Global Intelligence Working Group, http://it.ojp.gov/topic.jsp?topic_id=209
- DOJ's *National Criminal Intelligence Sharing Plan*, Global Intelligence Working Group, http://it.ojp.gov/topic.jsp?topic_id=93
- DOJ's *Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project*, Global Intelligence Working Group
- Organisation for Economic Co-operation and Development's (OECD) Fair Information Principles, http://it.ojp.gov/documents/OECD_FIPs.pdf

- Code of Federal Regulations (CFR), Title 28 (28 CFR)—Judicial Administration, Chapter 1—U.S. Department of Justice, Part 23—*Criminal Intelligence Systems Operating Policies,* http://it.ojp.gov/documents/28CFR_Part_23.pdf

- Office of the Program Manager, Information Sharing Environment (ISE), *Guidelines to Ensure That the Information Privacy and Other Legal Rights of Americans Are Protected in the Development and Use of the Information Sharing Environment* (ISE Privacy Guidelines), www.ise.gov/docs/privacy/PrivacyGuidelines20061204.pdf

- Office of the Program Manager, ISE, *An Introduction to the ISE Privacy Guidelines*, www.ise.gov/docs/privacy/ISEPrivacyGuidelinesIntroduction.pdf

- Office of the Program Manager, ISE, *Guideline 2—Develop a Common Framework for the Sharing of Information Between and Among Executive Departments and Agencies and State, Local, and Tribal Governments, Law Enforcement Agencies, and the Private Sector,* www.ise.gov/docs/guidance/guideline%202%20-%20common%20sharing%20framework.pdf

- Office of the Program Manager, ISE, *Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR), Version 1.5,* http://www.ise.gov/docs/ctiss/ISE-FS-200_ISE-SAR_Functional_Standard_V1_5_Issued_2009.pdf

- Office of the Program Manager, ISE, *ISE-SAR Privacy, Civil Rights, and Civil Liberties Protection Policy Template*

- Office of the Program Manager, ISE, Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI), www.ise.gov/pages/sar-initiative.aspx

Center personnel may also consider reviewing the following resources:

- Office of the Program Manager, ISE, *Privacy and Civil Liberties Implementation Guide for the Information Sharing Environment (ISE)*, www.ise.gov/docs/privacy/PrivacyImpGuide.pdf

- Federal Bureau of Investigation (FBI), Criminal Justice Information Services (CJIS) Division, *Privacy Impact Assessment of the Law Enforcement National Data Exchange (N-DEx)*, http://foia.fbi.gov/piandex040607.htm

Policy Development Template

A. Purpose Statement

Workbook Question

1. What is the purpose of establishing a privacy, civil rights, and civil liberties protection policy? (i.e., what does the center hope to accomplish in adopting this policy?) Provide a succinct, comprehensive statement of purpose.

Sample Language

Example 1:

1. The mission of the [name of center] is to collect, evaluate, analyze, and disseminate information and intelligence data (records) regarding criminal and terrorist activity in the [region or state] while following appropriate privacy and civil liberties safeguards as outlined in the principles of the Organisation for Economic Co-operation and Development's (OECD) Fair Information Principles to ensure that the information privacy and other legal rights of individuals and organizations are protected (see definitions of "Fair Information Principles" and "Protected Information" in [insert policy definitions section (see Appendix A, Terms and Definitions, of this template)]).

A. Purpose Statement

Workbook Question

Sample Language

Example 2:

1. The purpose of this privacy, civil rights, and civil liberties protection policy is to promote [name of center] and user conduct that complies with applicable federal, state, local, and tribal law [cite to policy definitions section (see Appendix A, Terms and Definitions, of this policy)] and assists the center and its users in:
   - Increasing public safety and improving national security.
   - Minimizing the threat and risk of injury to specific individuals.
   - Minimizing the threat and risk of physical or financial injury to law enforcement and others responsible for public protection, safety, or health.
   - Minimizing the threat and risk of damage to real or personal property.
   - Protecting individual privacy, civil rights, civil liberties, and other protected interests.
   - Protecting the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information.
   - Minimizing reluctance of individuals or groups to use or cooperate with the justice system.
   - Supporting the role of the justice system in society.
   - Promoting governmental legitimacy and accountability.
   - Not unduly burdening the ongoing business of the justice system.
   - Making the most effective use of public resources allocated to public safety agencies.

B. Policy Applicability and Legal Compliance

Workbook Question	Sample Language
1. Who is subject to the privacy policy? Identify who must comply with the policy; for example, center personnel, participating agencies, and private contractors.	1. All [name of center] personnel, participating agency personnel, personnel providing information technology services to the center, 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.
2. How is the center's policy made available to personnel, participating agencies, and individual users (in print, online, etc.), and are acknowledgment of receipt and agreement to comply with this policy required in writing?	2. The [name of center] will provide a printed or electronic copy of this policy to all center and non-center personnel who provide services and to participating agencies and individual users and will require both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and the applicable provisions it contains.
3. Does the center require ***personnel and participating information-originating and user agencies*** to be in compliance with all applicable constitutional and statutory laws protecting privacy, civil rights, and civil liberties in the gathering and collection, use, analysis, retention, destruction, sharing, disclosure, and dissemination of information? Cite the primary laws with which personnel and participating users must comply. This might include the U.S. and state constitutions; open records or sunshine laws; data breach notification laws; other laws, regulations, orders, opinions, or policies impacting or protecting privacy, civil rights, or civil liberties; local ordinances; and applicable federal laws and regulations, such as 28 CFR Part 23. (*Refer to Appendix B for a partial listing of primary federal laws relevant to seeking, retaining, and disseminating information at the federal level.*)	3. All [name of center] 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 laws protecting privacy, civil rights, and civil liberties, including, but not limited to [provide a list of applicable state and federal privacy, civil rights, and civil liberties laws].

B. Policy Applicability and Legal Compliance

Workbook Question

4. Does the center have ***internal operating policies*** that are in compliance with all applicable constitutional provisions and laws protecting privacy, civil rights, and civil liberties in the gathering and collection, use, analysis, retention, destruction, sharing, disclosure, and dissemination of information?

   Cite the primary laws with which internal operating policies must be in compliance.

Sample Language

4. The [name of center] has adopted internal operating policies that are in compliance with applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to [provide a listing of applicable state and federal privacy, civil rights, and civil liberties laws].

C. Governance and Oversight

Workbook Question	Sample Language
1. Who has primary responsibility for the center's overall operation, including the center's justice information systems, information collection and retention procedures, coordination of personnel, and enforcement of this policy? Which individual will ultimately be held accountable for the operation of the system and for any problems or errors?	1. Primary responsibility for the operation of the [name of center]; its justice systems, operations, and coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing, disclosure, or dissemination of information; and the enforcement of this policy is assigned to the [position/title] of the center.
2. Does the center have a privacy oversight committee or team that will develop the privacy policy and/or that will routinely review and update the policy?	2. The [name of center] is guided by a designated privacy oversight committee that liaises with the community 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 committee will annually review and update the policy in response to changes in law and implementation experience, including the results of audits and inspections.
3. Is there a designated and trained Privacy Officer who will handle reported errors and violations, oversee the implementation of privacy protections, and ensure that the center adheres to the provisions of the ISE Privacy Guidelines and other requirements for participation in the ISE? [Provide the title of the individual who will serve as the Privacy Officer, whether a full-time Privacy Officer position or the occupant of a different position, such as the Assistant Director or agency counsel.]	3. The [name of center]'s privacy committee is guided by a trained Privacy Officer [who is the (position) of the center and] who is appointed by the Director of the center. The Privacy Officer receives reports regarding alleged errors and violations of the provisions of this policy, receives and coordinates complaint resolution under the center's redress policy, 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 Officer can be contacted at the following address: [insert mailing address or e-mail address].
4. Who is responsible for ensuring that enforcement procedures and sanctions for noncompliance with the privacy policy are adequate and enforced?	4. The [name of center]'s Privacy Officer ensures that enforcement procedures and sanctions outlined in [insert section number of policy (see Section N.3, Enforcement, of this template)] are adequate and enforced.

D. Definitions

Workbook Question

1. What key words or phrases are regularly used in the policy for which the center wants to specify particular meanings?

   This may include terms that are not commonly known or have multiple meanings that may need to be clarified to indicate which one applies to the privacy policy. There may be legal definitions for terms in the statutes governing the operation of the justice information system. For examples of definitions of key terms commonly used throughout this template, refer to Appendix A.

Sample Language

1. For examples of primary terms and definitions used in this policy, refer to [insert section or appendix of policy (see Appendix A, Terms and Definitions, of this template)].

E. Information

Workbook Question

1. Identify what information ***may be*** sought, retained, shared, disclosed, or disseminated by the center.

   There may be different policy provisions for different types of information, such as tips and leads, SARs and ISE-SARs, criminal intelligence information, and fact-based information databases, such as criminal history records, case management information, deconfliction, wants and warrants, driver records, identification, and commercial databases.

   Best Practice: It is suggested that center policies include information that details the different types of information databases/ records that the center maintains or accesses and uses.

2. Identify what information ***may not*** be sought, retained, shared, or disclosed by the center.

   This may include federal or state constitutional prohibitions or prohibitions in federal, state, local, or tribal laws.

Sample Language

1. The [name of center] will seek or retain information that:
   - Is based on a possible threat to public safety or the enforcement of the criminal law, or
   - Is based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal (including terrorist) conduct or activity, or
   - 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 crime analysis or in the administration of criminal justice and public safety (including topical searches), and
   - The source of the information is reliable and verifiable or limitations on the quality of the information are identified, and
   - The information was collected in a fair and lawful manner, with the knowledge and consent of the individual, if appropriate.

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

2. The [name of center] will not seek or retain and information-originating agencies will agree not to submit information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, or sexual orientations.

E. Information

Workbook Question

3. Does your center apply labels to information (or ensure that the originating agency has applied labels) that indicate to the authorized user that:
   - The information is protected information as defined in the ISE Privacy Guidelines **or** as defined to include personal information on any individual regardless of citizenship or U.S. residency status? (Note: This definition may depend on state laws applicable to the collection and sharing of the information. See the definitions of "protected information" and "personal information" in Appendix A.) To what extent are organizations protected by the policy?
   - The information is subject to specific information privacy or other similar restrictions on access, use, or disclosure, and, if so, what is the nature of such restrictions? There may be laws that restrict who can access information, how information can be used, and limitations on the retention or disclosure of certain types of information; for example, the identity of a sexual assault victim.

4. Does your center categorize information (or ensure that the originating agency has categorized information) based on its nature (for example, tips and leads, suspicious activity reports, criminal history, intelligence information, case records, conditions of supervision, case progress), usability, and quality?

   The purpose of categorizing information is to assist users in:
   - Determining the quality and accuracy of the information.
   - Making the most effective use of the information.
   - Knowing whether and with whom the information can be appropriately shared.

Sample Language

3. The [name of center] applies labels to center-originated information (or ensures that the originating agency has applied labels) to indicate to the accessing authorized user that:
   - The information is protected information (as defined by the ISE Privacy Guidelines) [**or**] (as defined by the center to include personal information on any individual) [cite applicable authority, if any, and cite to center's definitions of "protected information" and "personal information" in Appendix A of policy], and, to the extent expressly provided in this policy, includes organizational entities.
   - The information is subject to [local, state or federal] laws restricting access, use, or disclosure.

4. The [name of center] personnel will, upon receipt of information, assess the information to determine or review its nature, usability, and quality. Personnel will assign categories to the information (or ensure that the originating agency has assigned categories to the information) to reflect the assessment, such as:
   - Whether the information consists of tips and leads data, suspicious activity reports, criminal history, intelligence information, case records, conditions of supervision, case progress, or other information category.
   - The nature of the source as it affects veracity (for example, anonymous tip, trained interviewer or investigator, public record, private sector).
   - The reliability of the source (for example, reliable, usually reliable, unreliable, unknown).
   - The validity of the content (for example, confirmed, probable, doubtful, cannot be judged).

E. Information

Workbook Question	Sample Language
5. When information is gathered or collected and retained by the center, is it labeled (by record, data set, or system of records), and are limitations assigned to identify who is allowed to see (access) and use the information (for example, credentialed, role-based levels of access)?	5. At the time a decision is made by the [name of center] to retain information, it will be labeled (by record, data set, or system of records), to the maximum extent feasible, pursuant to applicable limitations on access and sensitivity of disclosure to: • 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.
6. What conditions prompt the labels assigned in Section E.5 to be reevaluated?	6. The labels assigned to existing information under [insert section number of policy (see Section E.5 above)] 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.

E. Information

Workbook Question

7. If your center receives or collects ***tips and leads*** and/or ***suspicious activity report*** (SAR) information (information received or collected based on a level of suspicion that may be less than "reasonable suspicion"), does your center maintain and adhere to policies and procedures for:
   - Receipt and collection (information acquisition)—How the information is originally gathered, collected, observed, or submitted?
   - Assessment of credibility and value (organizational processing)—The series of manual and automated steps and decision points followed by the center to evaluate the SAR information?
   - Storage (integration and consolidation)—The point at which SAR information is placed into a SAR database, using a standard submission format, for purposes of permitting access by authorized personnel and agencies?
   - Access and dissemination (data retrieval and dissemination)—The process of making the information available to other agencies and obtaining feedback on investigative outcomes?
   - Retention and security of the information?

   Note: Some centers, based on state law or policy, use the "reasonable suspicion" standard as the threshold for sharing any information and intelligence containing personal information. If that is the case, the policy should so indicate.

Sample Language

7. [Name of center] personnel are required to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of tips and leads and 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 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 [insert retention period] in order to work an unvalidated tip, lead, or

E. Information

Workbook Question	Sample Language
	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. Does your center incorporate the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious activities and incidents (SAR process) into existing processes and systems used to manage other crime-related information and criminal intelligence?	8. The [name of center] 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. For purposes of sharing terrorism-related information through the ISE, has your center identified its data holdings that contain protected information (information about U.S. citizens or lawful permanent residents [constitutional minimum] or all individuals) to be shared through the ISE? [ISE information refers to terrorism-related information, which includes terrorism information, homeland security information, and law enforcement information related to terrorism.] Further, has your center put in place notice mechanisms, such as metadata or data field labels, for enabling ISE authorized users to determine the nature of the protected information that the center is making available in the ISE, such that participants can handle the information in accordance with applicable legal requirements? Refer to Appendix A for a definition of metadata.	9. The [name of center] will identify and review protected information that may be accessed from or disseminated by the center prior to sharing that information through the Information Sharing Environment. Further, the center will provide notice mechanisms, including but not limited to metadata or data field labels, that will enable ISE authorized users to determine the nature of the protected information and how to handle the information in accordance with applicable legal requirements. **Note:** The latter question needs to be addressed when a center opts **not** to provide notice mechanisms for all personal information such that users are able to determine the nature of the information and handle it in accordance with applicable legal requirements.

E. Information

Workbook Question	Sample Language
10. Does your center require certain basic descriptive information (metadata tags or labels) to be entered and associated with each record, data set, or system of records containing personally identifiable information that will be accessed, used, and disclosed, including terrorism-related information shared through the ISE? Basic information may include, where relevant and appropriate: • The name of the originating center or agency, department, component, and subcomponent (where applicable). • If applicable, the name of the center's justice information system from which the information is disseminated. • The date the information was collected (submitted) and, where feasible, the date its accuracy was last verified. • The title and contact information for the person to whom questions regarding the information, including its accuracy, should be directed.	10. The [name of center] 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 whom questions regarding the information should be directed.
11. Does your center attach (or ensure that the originating agency has attached) specific labels and descriptive information (metadata) to the information it collects and retains that clearly indicate legal restrictions on sharing of information based on information sensitivity or classification?	11. The [name of center] 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.
12. Does your center maintain a record of the source of the information sought and collected?	12. The [name of center] will keep a record of the source of all information sought and collected by the center.

F. Acquiring and Receiving Information

Workbook Question	Sample Language
1. Are there applicable state and federal constitutional provisions and statutes that govern or specify the techniques and methods the center may employ when seeking and receiving information? Identify and list these laws and provisions in the policy. Refer to Appendix B for a partial listing of primary federal laws relevant to seeking, retaining, or disseminating information at the federal level.	1. Information-gathering (acquisition) and access and investigative techniques used by the [name of center] and information-originating agencies will remain in compliance with and will adhere to applicable laws and guidance, including, but not limited to: • 28 CFR Part 23 regarding criminal intelligence information. • The OECD Fair Information Principles (under certain circumstances, there may be exceptions to the Fair Information Principles, based, for example, on authorities paralleling those provided in the federal Privacy Act; state, local, and tribal law; or center policy). • Criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) *National Criminal Intelligence Sharing Plan* (NCISP). • Constitutional provisions; [state] code, Section [insert number]; and administrative rules, as well as regulations and policies that apply to multijurisdictional intelligence and information databases.
2. Does your center's SAR process provide for human review and vetting to ensure that information is both legally gathered and, where applicable, determined to have a potential terrorism nexus? Are law enforcement officers and appropriate center and participating agency staff trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism?	2. The [name of center]'s SAR process provides for human review and vetting to ensure that information is both legally gathered and, where applicable, determined to have a potential terrorism nexus. Law enforcement officers and appropriate center and participating agency staff will be trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism.
3. Does your center's SAR process include 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?	3. The [name of center]'s SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved in activities that have been determined to be consistent with criminal activities associated with terrorism will be documented and shared through the ISE. These safeguards are intended to ensure that information that could violate civil rights (race, religion, national origin, ethnicity, etc.) and civil liberties (speech, assembly, religious exercise, etc.) will not be intentionally or inadvertently gathered, documented, processed, and shared.

F. Acquiring and Receiving Information

Workbook Question	Sample Language
4. Does the center (if an operational agency conducting investigations) adhere to a policy regarding the investigative techniques the center will follow when acquiring information (for example, an intrusion-level statement)?	4. Information-gathering and investigative techniques used by the [name of center] will and those used by originating agencies should be the least intrusive means necessary in the particular circumstances to gather information it is authorized to seek or retain.
5. Are agencies that access your center's information and/or share information with your center required to adhere to applicable law and policy?	5. External agencies that access the [name of center]'s information or share information with the center are governed by the laws and rules governing those individual agencies, including applicable federal and state laws.
6. If the center contracts with commercial databases, how does the center ensure that the commercial database entity is in legal compliance in its information-gathering techniques?	6. The [name of center] will contract only with commercial database entities that provide an assurance that their methods for gathering personally identifiable information comply with applicable local, state, tribal, territorial, and federal laws, statutes, and regulations and that these methods are not based on misleading information-gathering practices.
7. What are the types of information sources (nongovernmental, commercial, or private entities or institutions or classes of individuals) from which the center will not receive, seek, accept, or retain information?	7. The [name of center] 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 center policy. • An individual who or information provider that is legally prohibited from obtaining or disclosing the information.

G. Information Quality Assurance

Workbook Question	Sample Language
1. Does your center have established procedures and processes (manual and electronic) to ensure the quality (for example, accurate, complete, current, verifiable, and reliable) of the information it collects and maintains?	1. The [name of center] will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources; accurate; current; complete, including the relevant context in which it was sought or received and other related information; and merged with other information about the same individual or organization only when the applicable standard [refer to Section I, Merging Records, or appropriate policy section] has been met.
2. Does your center apply labels (or ensure that the originating agency has applied labels) to the information regarding its level of quality (for example, accurate, complete, current, verifiable, and reliable)?	2. At the time of retention in the system, the information will be labeled regarding its level of quality (accuracy, completeness, currency, and confidence [verifiability and reliability]).
3. Does your center research alleged or suspected errors and deficiencies (or refer them to the originating agency)? How does your center respond to confirmed errors or deficiencies?	3. The [name of center] investigates, in a timely manner, alleged errors and deficiencies (or refers them to the originating agency) and corrects, deletes, or refrains from using protected information found to be erroneous or deficient.
4. Does your center reevaluate (or ensure that the originating agency reevaluates) the labeling of information when new information is gathered that has an impact on the confidence (source reliability and content validity) in the information previously obtained?	4. The labeling of retained information will be reevaluated by the [name of center] or the originating agency when new information is gathered that has an impact on confidence (source reliability and content validity) in previously retained information.
5. When the center reviews the quality of the information it originates and identifies data that may be inaccurate or incomplete, includes incorrectly merged information, is out of date, cannot be verified, has a questionable source, or lacks adequate context such that the rights of the individual may be affected, what is the center's procedure for correction or destruction?	5. The [name of center] will conduct periodic data quality reviews of information it originates and make every reasonable effort to ensure that the information will be corrected, deleted from the system, or not used when the center identifies information that is erroneous, misleading, obsolete, or otherwise unreliable; the center did not have authority to gather the information or to provide the information to another agency; or the center used prohibited means to gather the information (except when the center's information source did not act as the agent of the center in gathering the information).

G. Information Quality Assurance

Workbook Question	Sample Language
6. When the center reviews the quality of the information it has received ***from*** an originating agency and identifies data that may be inaccurate or incomplete, includes incorrectly merged information, is out of date, cannot be verified, has a questionable source, or lacks adequate context such that the rights of the individual may be affected, does the center notify the originating agency or the originating agency's Privacy Officer? What method is used to notify the agency (written, telephone, or electronic notification)?	6. Originating agencies external to the [name of center] are responsible for reviewing the quality and accuracy of the data provided to the center. The center will review the quality of information it has received from an originating agency and advise the appropriate contact person in the originating agency, in writing or electronically, if its data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable.
7. When the center reviews the quality of the information it has ***provided to*** an external agency and identifies data that may be inaccurate or incomplete, includes incorrectly merged information, is out of date, cannot be verified, has a questionable source, or lacks adequate context such that the rights of the individual may be affected, does the center notify the external agency? What method is used to notify the agency (written, telephone, or electronic notification)?	7. The [name of center] will use written or electronic notification to inform recipient agencies when information previously provided to the recipient agency is deleted or changed by the center because the information is determined to be erroneous, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the rights of the individual may be affected.

H. Collation and Analysis

Workbook Question	Sample Language
1. Who is authorized (position/title, credentials, clearance level[s], etc.) to analyze information acquired or accessed by the center?	1. Information acquired or received by the [name of center] or accessed from other sources will be analyzed only by qualified individuals who have successfully completed a background check and appropriate security clearance, if applicable, and have been selected, approved, and trained accordingly.
2. What information is analyzed?	2. Information subject to collation and analysis is information as defined and identified in [Refer to Section E, Information, or appropriate policy section].
3. For what purpose(s) is the information analyzed? **Best Practice:** Does the center's Privacy Officer or privacy oversight committee review [and approve] all analytical products prior to dissemination or sharing by the center?	3. Information acquired or received by the [name of center] or accessed from other sources is analyzed according to priorities and needs and will be analyzed only to: • Further crime prevention (including terrorism), law enforcement, public safety, force deployment, or prosecution objectives and priorities established by the center. • Provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal (including terrorist) activities. **Best Practice Sample Language:** The [name of center] requires that all analytical products be reviewed [and approved] by the Privacy Officer [or privacy oversight committee] to ensure that they provide appropriate privacy, civil rights, and civil liberties protections prior to dissemination or sharing by the center.

I. Merging Records

Workbook Question

1. What matching criteria does your center require when attempting to merge information from multiple records allegedly about the same individual? In other words, when two records are compared for possible merger, are there certain attributes (name, fingerprint-based corrections number, date of birth, etc.) that must match, or is there a minimum number of attributes (for example, two out of five) that must match to link the two records as relating to the same person?

2. If the criteria specified in Section I.1 are not met, does the center have a procedure for partial matches?

Sample Language

Example 1:

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

Example 2:

1. The set of identifying information sufficient to allow merging by the [name of center] will utilize reasonable steps to identify the subject and may include the name (full or partial) and, in most cases, one or more of the following: date of birth; law enforcement or corrections system identification number; individual identifiers, such as fingerprints, photographs, physical description, height, weight, eye and hair color, race, ethnicity, tattoos, or scars; social security number; driver's license number; or other biometrics, such as DNA, retinal scan, or facial recognition. The identifiers or characteristics that, when combined, could clearly establish that the information from multiple records is about the same organization may include the name, federal or state tax ID number, office address, and telephone number.

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

J. Sharing and Disclosure

Workbook Question	Sample Language
1. What types of user actions and permissions are controlled by the center's access limitations? **Note:** User actions and permissions are often used to identify agencies and individuals with a need and right to know particular information or intelligence, access case management information, access non-personally identifiable information (PII) only, or to identify who is authorized to submit or modify particular records or record sets, to have read only access or to be authorized to add/modify/delete records, or to be authorized to grant privileges. **Best Practice:** It is suggested that centers specify their system for identifying user actions and permissions in their privacy policies.	1. Credentialed, role-based access criteria will be used by the [name of center], as appropriate, to control: • The information to which a particular group or class of users can have access based on the group or class. • The information a class of users can add, change, delete, or print. • To whom, individually, the information can be disclosed and under what circumstances.
2. For suspicious activity report information, does your center use a standard reporting format and commonly accepted data collection codes, and does the center's SAR information sharing process comply with the ISE Functional Standard for suspicious activity reporting? Refer to Section VIII., Resource List, within this template for a listing of SAR information resources, such as DOJ's *Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project* and Office of the Program Manager, ISE, *Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR)*, Version 1.5.	2. The [name of center] adheres to the current version of the ISE-SAR Functional Standard for its suspicious activity reporting (SAR) process, including the use of a standard reporting format and commonly accepted data collection codes and a sharing process that complies with the ISE-SAR Functional Standard for suspicious activity potentially related to terrorism.

J. Sharing and Disclosure

Workbook Question	Sample Language
3. Describe the conditions and credentials by which access to and disclosure of records retained by the center will be provided ***within the center or in other governmental agencies***. Is an audit trail kept of access to and disclosure of information retained by the center (e.g., dissemination logs, algorithms)? Refer to N.2, Accountability, for more information on audit logs.	3. Access to or disclosure of records retained by the [name of center] will be provided only ***to persons within the center or in other governmental agencies*** who are authorized to have access and only for legitimate law enforcement, public protection, public prosecution, public health, or justice purposes and only for the performance of official duties in accordance with law and procedures applicable to the agency for which the person is working. An audit trail sufficient to allow the identification of each individual who accessed information retained by the center and the nature of the information accessed will be kept by the center.
4. Are participating agencies that access information from your center required to obtain approval from the originator of the information prior to further dissemination or to follow the disclosure law applicable to the originating agency?	4. Agencies external to the [name of center] may not disseminate information accessed or disseminated from the center without approval from the center or other originator of the information.
5. Describe the conditions under which access to and disclosure of records retained by the center will be provided ***to those responsible for public protection, public safety, or public health***. Is an audit trail kept of access to and disclosure of information retained by the center (e.g., dissemination logs, algorithms)? Refer to N.2, Accountability, for more information on audit logs.	5. Records retained by the [name of center] 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.
6. Describe the conditions under which access to and disclosure of records retained by the center will be provided ***for specific purposes*** in response to requests by persons authorized by law. Is an audit trail kept of access to and disclosure of information retained by the center (e.g., dissemination logs, algorithms)? Refer to N.2, Accountability, for more information on audit logs.	6. Information gathered or collected and records retained by the [name of center] may be accessed or disseminated ***for specific purposes*** upon request by persons authorized by law to have such access and only for those uses and purposes specified in the law. 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 [specify the retention period for your jurisdiction for this type of request] by the center.

J. Sharing and Disclosure

Workbook Question	Sample Language
7. Under what circumstances will access to and disclosure of a record be provided ***to a member of the public*** in response to an information request, and are these circumstances described in your center's redress policy? Is an audit trail kept of disclosure of information retained by the center (e.g., dissemination logs, algorithms)? Refer to N.2, Accountability, for more information on audit logs. **Note:** This issue does not apply to circumstances in which a center chooses to provide nonsensitive information to the public or to provide sensitive information in accordance with center policy in response to an emergency situation.	7. Information gathered or collected and records retained by the [name of center] may be accessed or disclosed ***to a member of the public*** only if the information is defined by law to be a public record or otherwise appropriate for release to further the center's mission and is not exempt from disclosure by law. Such information may be disclosed only in accordance with the law and procedures applicable to the center for this type of information. An audit trail sufficient to allow the identification of each individual member of the public who accessed or received information retained by the center and the nature of the information accessed will be kept by the center.
8. Under what circumstances and to whom will the center ***not disclose*** records and information?	8. Information gathered or collected and records retained by the [name of center] ***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.

J. Sharing and Disclosure

Workbook Question

9. What are the categories of records that will ordinarily ***not be provided*** to the public pursuant to applicable legal authority?

10. State the center's policy on confirming the existence or nonexistence of information to persons or agencies that are not eligible to receive the information.

Sample Language

9. There are several categories of records that will ordinarily ***not be provided*** to the public:
   - Records required to be kept confidential by law are exempted from disclosure requirements under [**cite public records act and applicable section**].
   - Information that meets the definition of "classified information" as that term is defined in the National Security Act, Public Law 235, Section 606.
   - Investigatory records of law enforcement agencies that are exempted from disclosure requirements under [**cite public records act and applicable section**]. However, certain law enforcement records must be made available for inspection and copying under [**cite public records act and applicable section**].
   - 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 [**cite public records act and applicable section**]. This includes a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism under [**cite public records act and applicable section**] or an act of agricultural terrorism under [**cite public records act and applicable section**], vulnerability assessments, risk planning documents, needs assessments, and threat assessments.
   - Protected federal, state, local, or tribal records, which may include records originated and controlled by another agency that cannot, under [**cite applicable law**], be shared without permission.
   - A violation of an authorized nondisclosure agreement under [**cite applicable law**].

10. The [name of center] shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information unless otherwise required by law.

K. Redress

Workbook Question

K.1 Disclosure

1. If required by state statute, what are the conditions under which the center will disclose information to an individual about whom information has been gathered? Is a record kept of all requests and of what information is disclosed to an individual?

   Note: If the state public (open) records act provides procedures for disclosure, corrections, appeals, and handling of complaints when information is not subject to disclosure, these procedures should be summarized in the policy in lieu of using the sample language provided.

2. What are the conditions under which the center will not disclose information to an individual about whom information has been gathered? Does the center refer the individual to the agency originating the information?

Sample Language

1. Upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity and subject to the conditions specified in 2., below, an individual is entitled to know the existence of and to review the information about him or her that has been gathered and retained by the [name of center]. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information (correction). The center's response to the request for information will be made within a reasonable time and in a form that is readily intelligible to the individual. A record will be kept of all requests and of what information is disclosed to an individual.
2. The existence, content, and source of the information will not be made available by the [name of center] to an individual when [**the policy must cite applicable legal authority for each stated basis for denial**]:
   - Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution.
   - Disclosure would endanger the health or safety of an individual, organization, or community.
   - The information is in a criminal intelligence information system subject to 28 CFR Part 23 [see 28 CFR § 23.20(e)].
   - The information relates to [title, regulation, or code, etc.].
   - The information source does not reside with the center.
   - The center did not originate and does not have a right to disclose the information.
   - Other ***authorized*** basis for denial.

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

K. Redress

Workbook Question	Sample Language
K.2 Corrections	
1. What is the center's procedure for handling individuals' requests for correction involving ***information the center has disclosed and can change because it originated the information***? Is a record kept of requests for corrections?	1. If an individual requests correction of information ***originating with the [name of center]*** that has been disclosed, the center's Privacy Officer or designee will inform the individual of the procedure for requesting and considering requested corrections, including appeal rights if requests are denied in whole or in part. A record will be kept of all requests for corrections and the resulting action, if any.
K.3 Appeals	
1. If requests for disclosure or corrections are denied, what is the center's procedure for appeal?	1. 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 [name of center] or the originating agency. The individual will also be informed of the procedure for appeal when the center or originating agency has cited an exemption for the type of information requested or has declined to correct challenged information to the satisfaction of the individual to whom the information relates.
K.4 Complaints	
1. For terrorism-related protected information that may be accessed or shared through the ISE, what is the center's process for handling individuals' complaints and objections with regard to information received, maintained, disclosed, or disseminated by the center? Is the center's ISE Privacy Officer or designee or other individual responsible for handling complaints? Is a record kept of complaints and requests for corrections? **Best Practice:** Centers are encouraged to make the complaint procedure applicable to all information and intelligence held by the center that is exempt from disclosure and correction procedures, in which case it would not be necessary to address Section K.4, 2 (see Note for Section K.4, 2.).	1. If an individual has a complaint with regard to the accuracy or completeness of terrorism-related protected information that: (a) Is exempt from disclosure, (b) Has been or may be shared through the ISE, (1) Is held by the [name of center] and (2) Allegedly has resulted in demonstrable harm to the complainant, The center will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the center's Privacy Officer or [insert title of designee or other individual] at the following address: (insert mailing address, e-mail address, and/or link to page if complaints can be submitted electronically). The Privacy Officer or [insert title of designee or other individual] 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

K. Redress

Workbook Question	Sample Language
	by law. If the information did not originate with the center, the Privacy Officer or [insert title of designee or other individual] will notify the originating agency in writing or electronically within 10 days and, upon request, assist such agency to correct any identified data/record deficiencies, purge the information, or verify that the record is accurate. All information held by the center that is the subject of a complaint will be reviewed within 30 days and confirmed or corrected/purged if determined to be inaccurate or incomplete, to include incorrectly merged information, or to be out of date. If there is no resolution within 30 days, the center will not share the information until such time as the complaint has been resolved. A record will be kept by the center of all complaints and the resulting action taken in response to the complaint.
2. How does the center determine which complaints involve information that is specifically protected information shared through the ISE? **Note:** This question needs to be addressed when a center does not have a procedure applicable to all protected information under Section K.4, 1.	2. To delineate protected information shared through the ISE from other data, the [name of center] maintains records of agencies sharing terrorism-related information and employs system mechanisms to identify the originating agency when the information is shared.

L. Security Safeguards

Workbook Question	Sample Language
1. Does your center have a designated security officer? Is training provided for the security officer? If the role is a component of another position, identify the title of the position upholding security officer responsibilities.	1. The [name of center]'s [insert position title] is designated and trained to serve as the center's security officer.
2. What are your center's physical, procedural, and technical safeguards for ensuring the security of center data? Describe how the center will protect the information from unauthorized access, modification, theft, or sabotage (whether internal or external) resulting from natural or human-caused disasters or intrusions with, for example, procedures, practices, system protocols, use of software, information technology tools, and physical security measures. **Best Practice:** Reference generally accepted industry or other applicable standard(s) for security with which the center complies.	2. The [name of center] will operate in a secure facility protected from external intrusion. The center will utilize secure internal and external safeguards against network intrusions. Access to the center's databases from outside the facility will be allowed only over secure networks.
3. Does your center utilize a separate repository system for tips, leads, and SAR information?	3. The [name of center] will secure tips, leads, and SAR information in a separate repository system using security procedures and policies that are the same as or similar to those used for a system that secures data rising to the level of reasonable suspicion under 28 CFR Part 23.
4. What requirements exist to ensure that the information will be stored in a secure format and a secure environment?	4. The [name of center] 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.
5. What are the required credentials of center personnel authorized to have access to center information?	5. Access to [name of center] information will be granted only to center personnel whose positions and job duties require such access; who have successfully completed a background check and appropriate security clearance, if applicable; and who have been selected, approved, and trained accordingly.
6. Does electronic access to center data identify the user?	6. Queries made to the [name of center]'s data applications will be logged into the data system identifying the user initiating the query.

L. Security Safeguards

Workbook Question

7. Is a log kept of accessed and disseminated center data, and is an audit trail maintained? Refer to N.2, Accountability, for more information on audit logs.
8. Are risk and vulnerability assessments (if maintained) stored separately from publicly available data?
9. What are the center's procedures for adhering to data breach notification laws or policies?

Best Practice: Provide notification to originating agencies when personal information they provided to the center has been the subject of a suspected or confirmed data breach.

Sample Language

7. The [name of center] will utilize watch logs to maintain audit trails of requested and disseminated information.
8. To prevent public records disclosure, risk and vulnerability assessments will not be stored with publicly available data.

Option 1:

9. [If there is no applicable data breach notification law and you choose not to follow the OMB guidance in Option 2.] The [name of 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 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.

Option 2:

9. [If there is no applicable data breach notification law and you choose to follow the OMB guidance.] The [name of center] will follow the data breach notification guidance set forth in OMB Memorandum M-07-16 (May 2007, see http://www.whitehouse.gov/OMB/memoranda/fy2007/m07-16.pdf).

Option 3:

9. [If there is an applicable data breach notification law.] The [name of center] will follow the data breach notification guidance set forth in [**cite to applicable law**].

Best Practice Sample Language: [To the extent allowed by the (state) data breach notification law] The [name of center] will immediately notify the originating agency from which the center received personal information of a suspected or confirmed breach of such information.

M. Information Retention and Destruction

Workbook Question

1. What is your center's review schedule for validating or purging information? Specify periodic basis and/or reference the applicable law.

   Note: Retention and destruction policy should be provided for all information and intelligence databases/records held by the center.

2. Does your center have a retention and destruction policy? Reference laws, if applicable.

3. What methods are employed by the center to remove or destroy information?

4. Is approval needed prior to removal or destruction of information? Specify the law, statute, regulation, or policy, if applicable, requiring that permission must be obtained before destroying information or specify that no approval will be required.

5. Is the source of the information notified prior to removal or destruction?

Sample Language

1. All applicable information will be reviewed for record retention (validation or purge) by [name of center] at least every five (5) years, as provided by 28 CFR Part 23 [or for a longer or shorter period as specified by state law or local ordinance].

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

3. The [name of center] will delete information or return it to the originating agency once its retention period has expired as provided by this policy or as otherwise agreed upon with the originating agency in a participation or membership agreement.

Option 1:

4. The procedure contained in [cite law, statute, regulation, or policy] will be followed by [name of center] for notification of appropriate parties, including the originating agency, before information is deleted or returned in accordance with this policy or as otherwise agreed upon with the originating agency in a participation or membership agreement.

Option 2:

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

5. Notification of proposed destruction or return of records may or may not be provided to the originating agency by the [name of center], depending on the relevance of the information and any agreement with the originating agency.

M. Information Retention and Destruction

Workbook Question	Sample Language
6. Is a record kept of dates when information is to be removed (purged) if not validated prior to the end of its period? Is notification given prior to removal (for example, an autogenerated system prompt to center personnel that a record is due for review and validation or purge)?	6. A record of information to be reviewed for retention will be maintained by the [name of center], and for appropriate system(s), notice will be given to the submitter at least 30 days prior to the required review and validation/purge date.

N. Accountability and Enforcement

Workbook Question	Sample Language
N.1 Information System Transparency	
1. Is your center's privacy policy available to the public?	1. The [name of 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, made available upon request, and posted on the center's Web site [or Web page] at (insert Web address).
2. Does your center have a point of contact for handling inquiries or complaints?	2. The [name of center]'s [Privacy Officer **or** other position title] 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 **or** other position title] can be contacted at [insert mailing address or e-mail address].
N.2 Accountability	
1. Does electronic access (portal) to the center's data identify the user? Is the identity of the user retained in the audit log?	1. The audit log of queries made to the [name of center] will identify the user initiating the query.
2. Is a log kept of accessed and disseminated center-held data, and is an audit trail maintained?	2. The [name of center] will maintain an audit trail of accessed, requested, or disseminated information. An audit trail will be kept for a minimum of [specify the retention period for your jurisdiction/center for this type of request] of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.
3. What procedures and practices does your center follow to enable evaluation of user compliance with system requirements, the center's privacy policy, and applicable law?	3. The [name of center] will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with system requirements and with the provisions of this policy and applicable law. This will include logging access to these systems and periodic auditing of these systems, so as to not establish a pattern of the audits. These audits will be mandated at least [quarterly, semiannually, or annually] and a record of the audits will be maintained by the [Privacy Officer or title of designee] of the center.

N. Accountability and Enforcement

Workbook Question	Sample Language
4. Does your center have a mechanism for personnel to report errors and violations of center policies related to protected information?	4. The [name of center]'s personnel or other authorized users shall report errors and suspected or confirmed violations of center policies relating to protected information to the center's Privacy Officer. [Cross-reference to policy (see Section C.3 of this template).]
5. Are audits completed by an independent third party or a designated representative of the center? Are the audits conducted both annually and randomly?	5. The [name of center] 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 center's [designate audit committee, office, or position] (or) [a designated independent panel]. This [committee/office/position] (or) [independent panel] has the option of conducting a random audit, without announcement, at any time and without prior notice to staff of the center. The audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the center's information and intelligence system(s).
6. How often do you review and update the provisions contained within this privacy policy (for example, annually)?	6. The [name of center]'s privacy committee, 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.

N. Accountability and Enforcement

Workbook Question

N.3 Enforcement

1. What are your procedures for enforcement if center personnel, a participating agency, or an authorized user is suspected of being or has been found to be in noncompliance with the provisions of this policy?

2. What is the center's policy with regard to the qualifications and number of participating agency personnel authorized to access center information and intelligence, and what additional sanctions are available for violations of the center's privacy policy?

Sample Language

1. If center personnel, a participating agency, or an authorized user is found to be in noncompliance with the provisions of this policy regarding the gathering, collection, use, retention, destruction, sharing, classification, or disclosure of information, the [title of center Director] of the [name of center] will:
   - Suspend or discontinue access to information by the center personnel, the participating agency, or the authorized user.
   - Suspend, demote, transfer, or terminate center personnel, as permitted by applicable personnel policies.
   - Apply administrative actions or sanctions as provided by [state agency or center] rules and regulations or as provided in agency/center personnel policies.
   - If the authorized user is from an agency external to the agency/center, request that the relevant agency, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions.
   - Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

2. The [name of center] 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.

O. Training

Workbook Question	Sample Language
1. What personnel does your center require to participate in training programs regarding implementation of and adherence to this privacy policy?	1. The [name of center] will require the following individuals to participate in training programs regarding implementation of and adherence to the privacy, civil rights, and civil liberties policy: • All assigned personnel of the center. • Personnel providing information technology services to the center. • Staff in other public agencies or private contractors providing services to the center. • Users who are not employed by the center or a contractor.
2. Do you provide training to personnel authorized to share protected information through the ISE?	2. The [name of center] will provide special training regarding the center's requirements and policies for collection, use, and disclosure of protected information to personnel authorized to share protected information through the Information Sharing Environment.
3. What is covered by your training program (for example, purpose of the policy, substance and intent of the provisions of the policy, impact of infractions, and possible penalties for violations)?	3. The [name of 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. • Originating and participating agency responsibilities and obligations under applicable law and policy. • How to implement the policy in the day-to-day work of the user, whether a paper or systems user. • The impact of improper activities associated with infractions within or through the agency. • Mechanisms for reporting violations of center privacy protection policies and procedures. • The nature and possible penalties for policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.

Appendix A
Terms and Definitions

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 center's 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. Data access is usually specified as read-only and read/write access.

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

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

Acquisition—The means by which an ISE participant obtains information through the exercise of its authorities; for example, through human intelligence collection or from a foreign partner. For the 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—The [name of agency] and all agencies that access, contribute, and share information in the [name of agency]'s justice information system.

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

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

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

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

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

Center—Refers to the [name of fusion center] and all participating state agencies of the [name of fusion center].

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

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

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

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

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

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

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

Data Breach—The unintentional release of secure information to an untrusted environment. This may include incidents such as theft or loss of digital media—including computer tapes, hard drives, or laptop computers containing such media—upon which such information is stored unencrypted; posting such information on the World Wide Web or on a computer otherwise accessible from the Internet without proper information security precautions; transfer of such information to a system that is not completely open but is not appropriately or formally accredited for security at the approved level, such as unencrypted e-mail; or transfer of such information to the information systems of a possibly hostile agency or environment where it may be exposed to more intensive decryption techniques.

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

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

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

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

Fair Information Principles—The Fair Information Principles (FIPs) are contained within the 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:

- Collection Limitation Principle
- Data Quality Principle
- Purpose Specification Principle
- Use Limitation Principle
- Security Safeguards Principle
- Openness Principle
- Individual Participation Principle
- Accountability Principle

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

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

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

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

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

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

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

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

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

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

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

Law Enforcement Information—For purposes of the ISE, law enforcement information means any information obtained by or of interest to a law enforcement agency or

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

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

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

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

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

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

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

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

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

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

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

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

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

Personal characteristics (such as height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation, place of birth, mother's maiden name, distinguishing features, and biometrics information, such as fingerprints, DNA, and retinal scans).

A unique set of numbers or characters assigned to a specific individual (including name, address, phone number, social security number, e-mail address, driver's license number, financial account or credit card number and associated PIN number, Integrated Automated Fingerprint Identification System [IAFIS] identifier, or booking or detention system number).

Descriptions of event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records).

Descriptions of location(s) or place(s) (including geographic information systems [GIS] locations, electronic bracelet monitoring information, etc.).

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

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

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

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

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

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

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

Public—Public includes:

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

Public does not include:

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

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

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

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

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

Retention—Refer to Storage.

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

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

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

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

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

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

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 is probably the most common meaning in the IT industry.

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—including homeland security information, terrorism information, and law enforcement information relating to terrorism or the security of our homeland—by both the originator of the information and any recipient of the information.

Suspicious Activity—Defined in the ISE-SAR Functional Standard (Version 1.5) as "observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity." Examples of suspicious activity include surveillance, photography of sensitive infrastructure facilities, site breach or physical intrusion, cyberattacks, 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 the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), all information relating to (a) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or materials support, or activities of foreign **or** international terrorist groups or individuals **or** of domestic groups **or** individuals involved in transnational terrorism; (b) threats posed by such groups or individuals to the United States, United States persons, or United States interests or to those interests of other nations; (c) communications of or by such groups or individuals; or (d) other groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

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

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

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

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

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

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

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.ise.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 an 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 1, Part 23

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Appendix C
Suspicious Activity Reporting (SAR) Summary of Provisions

For fusion centers that are continuing to formulate or may have already completed a privacy policy using this template prior to the inclusion of SAR provisions, a summary of the updated provisions specific to the SAR process is provided within this appendix. Section headings and numbering are retained for template reference purposes. Please note that other provisions contained within this template may also apply to SAR information.

E. Information

Workbook Question

1. Identify what information ***may be*** sought, retained, shared, disclosed, or disseminated by the center.

   There may be different policy provisions for different types of information, such as tips and leads, SARs and ISE-SARs, criminal intelligence information, and fact-based information databases, such as criminal history records, case management information, deconfliction, wants and warrants, driver records, identification, and commercial databases.

   Best Practice: It is suggested that center policies include information that details the different types of information databases/ records that the center maintains or accesses and uses.

Sample Language

1. The [name of center] will seek or retain information that:
   - Is based on a possible threat to public safety or the enforcement of the criminal law, or
   - Is based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal (including terrorist) conduct or activity, or
   - 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 crime analysis or in the administration of criminal justice and public safety (including topical searches), and
   - The source of the information is reliable and verifiable or limitations on the quality of the information are identified, and
   - The information was collected in a fair and lawful manner, with the knowledge and consent of the individual, if appropriate.

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

E. Information

Workbook Question	Sample Language
4. Does your center categorize information (or ensure that the originating agency has categorized information) based on its nature (for example, tips and leads, suspicious activity reports, criminal history, intelligence information, case records, conditions of supervision, case progress), usability, and quality? The purpose of categorizing information is to assist users in: • Determining the quality and accuracy of the information. • Making the most effective use of the information. • Knowing whether and with whom the information can be appropriately shared.	4. The [name of center] personnel will, upon receipt of information, assess the information to determine or review its nature, usability, and quality. Personnel will assign categories to the information (or ensure that the originating agency has assigned categories to the information) to reflect the assessment, such as: • Whether the information consists of tips and leads data, suspicious activity reports, criminal history, intelligence information, case records, conditions of supervision, case progress, or other information category. • The nature of the source as it affects veracity (for example, anonymous tip, trained interviewer or investigator, public record, private sector). • The reliability of the source (for example, reliable, usually reliable, unreliable, unknown). • The validity of the content (for example, confirmed, probable, doubtful, cannot be judged).
7. If your center receives or collects ***tips and leads*** and/or ***suspicious activity report*** (SAR) information (information received or collected based on a level of suspicion that may be less than "reasonable suspicion"), does your center maintain and adhere to policies and procedures for: • Receipt and collection (information acquisition)—How the information is originally gathered, collected, observed, or submitted? • Assessment of credibility and value (organizational processing)—The series of manual and automated steps and decision points followed by the center to evaluate the SAR information? • Storage (integration and consolidation)—The point at which SAR information is placed into a SAR database, using a standard submission format, for purposes of permitting access by authorized personnel and agencies?	7. [Name of center] personnel are required to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of tips and leads and 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.

E. Information

Workbook Question

Question 7 (continued)

- Access and dissemination (data retrieval and dissemination)—The process of making the information available to other agencies and obtaining feedback on investigative outcomes?
- Retention and security of the information?

Note: Some centers, based on state law or policy, use the "reasonable suspicion" standard as the threshold for sharing any information and intelligence containing personal information. If that is the case, the policy should so indicate.

Sample Language

Sample Language 7 (continued)

- 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 [insert retention period] 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.

E. Information

Workbook Question	Sample Language
8. Does your center incorporate the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious activities and incidents (SAR process) into existing processes and systems used to manage other crime-related information and criminal intelligence?	8. The [name of center] 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.

F. Acquiring and Receiving Information

Workbook Question	Sample Language
2. Does your center's SAR process provide for human review and vetting to ensure that information is both legally gathered and, where applicable, determined to have a potential terrorism nexus? Are law enforcement officers and appropriate center and participating agency staff trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism?	2. The [name of center]'s SAR process provides for human review and vetting to ensure that information is both legally gathered and, where applicable, determined to have a potential terrorism nexus. Law enforcement officers and appropriate center and participating agency staff will be trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism.
3. Does your center's SAR process include 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?	3. The [name of center]'s SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved in activities that have been determined to be consistent with criminal activities associated with terrorism will be documented and shared through the ISE. These safeguards are intended to ensure that information that could violate civil rights (race, religion, national origin, ethnicity, etc.) and civil liberties (speech, assembly, religious exercise, etc.) will not be intentionally or inadvertently gathered, documented, processed, and shared.

J. Sharing and Disclosure

Workbook Question	Sample Language
2. For suspicious activity report information, does your center use a standard reporting format and commonly accepted data collection codes, and does the center's SAR information sharing process comply with the ISE Functional Standard for suspicious activity reporting? Refer to the Resource List within this template for a listing of SAR information resources, such as DOJ's *Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project* and Office of the Program Manager, ISE, *Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR)*, Version 1.5.	2. The [name of center] adheres to the current version of the ISE-SAR Functional Standard for its suspicious activity reporting (SAR) process, including the use of a standard reporting format and commonly accepted data collection codes and a sharing process that complies with the ISE-SAR Functional Standard for suspicious activity potentially related to terrorism.

L. Security Safeguards

3. Does your center utilize a separate repository system for tips, leads, and SAR information?	3. The [name of center] will secure tips, leads, and SAR information in a separate repository system using security procedures and policies that are the same as or similar to those used for a system that secures data rising to the level of reasonable suspicion under 28 CFR Part 23.

Appendix A—Terms and Definitions

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

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

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

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

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

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