United States
Department of Justice

Privacy, Civil Rights, and Civil Liberties

Policy Development Template

for State, Local, and Tribal Justice Entities

April 2012


We the People
insure domestic Tranquility, provide for the
and our Posterity, do ordain and establish

Privacy, Civil Rights, and Civil Liberties Policy Development Template for State, Local, and Tribal Justice Entities

Where to Locate This Resource

This resource is available online at www.it.ojp.gov/privacy. To request printed copies, send requests to GLOBAL@iir.com.

To Request a Word Version of the Template

To request a Word version, send requests to GLOBAL@iir.com.

About Global

www.it.ojp.gov/global

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

Global supports the initiatives of DOJ and aids Global member organizations and the people they serve through a series of important collaborative efforts. These include the facilitation of Global working groups.

About GPIQWG

www.it.ojp.gov/gpiqwg

The Global Privacy and Information Quality Working Group (GPIQWG) is one of five Global working groups. GPIQWG is a cross-functional, multidisciplinary working group of Global and is composed of privacy and local, state, tribal, and federal justice entity representatives covering critical topics such as intelligence, biometrics, information quality, privacy, civil rights, and civil liberties. GPIQWG assists government entities, institutions, and other justice agencies in ensuring that personally identifiable information is appropriately collected, maintained, used, and disseminated within evolving integrated justice information systems.

GPIQWG, on behalf of DOJ's Global, developed this template to support justice agencies in their efforts to balance the interests of law enforcement and public safety with the privacy rights and concerns of affected persons. For more information on GPIQWG, refer to: www.it.ojp.gov/gpiqwg.

This project was supported by Grant No. 2010-MU-BX-K019 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. 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.

Table of Contents

Introduction

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 entities and individuals can exercise discretion in deciding how to proceed. Entities 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 template is provided to assist entity personnel in developing a privacy policy related to the information the entity collects, receives, maintains, archives, accesses, and discloses to entity personnel; governmental agencies; fusion centers; Information Sharing Environment (ISE) participants, on behalf of fusion centers; 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 entity's general operational policies and day-to-day operations and to provide explicit and detailed privacy protection guidance to entity 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 (IQ), collation and analysis, merging of records, information access and disclosure, redress, security safeguards, retention and destruction, accountability and enforcement, and training.

A. How to Use This Template

This template is designed with privacy policy concepts grouped into related sections. Each section contains pertinent policy provision questions shown in **bold** type, followed by useful policy sample language. Sections containing **"informational only"** Information Sharing Environment (ISE) components are boxed, and sections containing suspicious activity reporting (SAR) components are shaded.

Frequently, entities already have established privacy-related policies and practices contained 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, entities 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. Entities are cautioned, however, against simply providing a cross-reference to other policies in effect. Cross-referencing, without including the applicable policy language, should be done only if those policies are also available to the public; otherwise, entities should restate the applicable language in their privacy policies.

B. 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 entity, 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 entity to establish minimum baseline privacy protections. Entities 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.

C. References to the Information Sharing Environment (ISE) and Fusion Centers

This template was originally designed as a tool to assist fusion centers in the development of their privacy, civil rights, and civil liberties protection policies. As such, Information Sharing Environment (ISE) concepts, as they relate to fusion centers or other state, local, and tribal (SLT) entities receiving terrorism-related information directly from or providing information directly to federal entities, were integrated throughout each section. ISE concepts were retained **"for informational purposes only"** to educate readers on how the information an entity collects may be held to requirements at least as comprehensive as the ISE Privacy Guidelines in the future (for example, if entity information is shared with or distributed through a fusion center). To distinguish ISE components from broader SLT-related policy concepts, ISE components are boxed. For more information on the ISE, refer to 1. and 2., below.

1. 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 in the development and operation of the ISE.

2. The ISE and Fusion Centers

According to the ISE Privacy Guidelines, "Protected information [see Appendix A, Glossary of 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, entities 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 entity terrorism-related information. The ISE Privacy Guidelines stipulate "that such non-federal 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."

D. 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, Civil Rights, and Civil Liberties Policy Development Guide for State, Local, and Tribal Justice Entities*, Global Justice Information Sharing Initiative's (Global) Privacy and Information Quality Working Group, http://it.ojp.gov/Privacy.
- 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.
- DOJ's Global Intelligence Working Group Privacy Committee, Tips and Leads Issue Paper
- 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/sites/default/files/PrivacyGuidelines20061204.pdf.
- Office of the Program Manager, ISE, *An Introduction to the ISE Privacy Guidelines*, www.ise.gov/sites/default/files/ISEPrivacyGuidelinesIntroduction_0.pdf.
- Office of the Program Manager, ISE, *Guideline 2—Develop a Common Framework for the Sharing of Information Between and Among Executive Departments and Entities and State, Local, and Tribal Governments, Law Enforcement Entities, and the Private Sector*, www.ise.gov/sites/default/files/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*, www.ise.gov/sites/default/files/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/nationwide-sar-initiative.

Entity personnel may also consider reviewing the following resources:

- Office of the Program Manager, ISE, *ISE Privacy Guidelines Implementation Manual*, www.ise.gov/ise-privacy-guidelines-implementation-manual and www.ise.gov/sites/default/files/PrivacyImpGuide_0.pdf.
- Federal Bureau of Investigation (FBI), Criminal Justice Information Services (CJIS) Division, *Privacy Impact Assessment of the Law Enforcement National Data Exchange (N-DEx)*, www.fbi.gov/about-us/cjis/n-dex/piandex.

Policy Development Template

A. Purpose Statement

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

Example 1:

The mission of the [name of entity] 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 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, Glossary of Terms and Definitions)]).

Example 2:

The purpose of this privacy, civil rights, and civil liberties protection policy is to promote [name of entity] and user conduct that complies with applicable federal, state, local, and tribal law [cite to policy definitions section (see Appendix A, Glossary of Terms and Definitions)] and assists the entity 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 entities.

B. Policy Applicability and Legal Compliance

1. Who is subject to the privacy policy?

Identify who must comply with the policy; for example, entity personnel, participating agencies, and private contractors.

All [name of entity] personnel, participating agency personnel, personnel providing information technology services to the entity, private contractors, and other authorized users will comply with the entity's privacy policy. This policy applies to information the entity gathers or collects, receives, maintains, stores, accesses, discloses, or disseminates to entity personnel, governmental agencies (including Information Sharing Environment [ISE] participating agencies), and participating justice and public safety agencies, as well as to private contractors, private agencies, and the general public.

2. How is the entity's policy made available to personnel, participating entities, and individual users (in print, online, etc.), and are acknowledgment of receipt and agreement to comply with this policy required in writing?

The [name of entity] will provide a printed or electronic copy of this policy to all entity and nonentity 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 entity 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. Constitution 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. (For synopses of primary federal laws an agency should review for including in the privacy policy, refer to Appendix B, Federal Laws Relevant to Seeking, Retaining, and Disseminating Justice Information.)

All [name of entity] personnel, participating agency personnel, personnel providing information technology services to the entity, private contractors, agencies from which entity 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].

4. Does the entity 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.

The [name of entity] 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 list of applicable state and federal privacy, civil rights, and civil liberties laws].

C. Governance and Oversight

1. **Who has primary responsibility for the entity's overall operation, including the entity'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?**

   Primary responsibility for the operation of the [name of entity]; its justice systems, operations, and coordination of personnel; the receiving, seeking, retention, evaluation, IQ, analysis, destruction, sharing, disclosure, or dissemination of information; and the enforcement of this policy is assigned to the [position/title] of the entity.

2. **Does the entity have a privacy oversight committee or team that will develop the privacy policy and/or that will routinely review and update the policy?**

   The [name of entity] 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 entity'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 and oversee the implementation of privacy protections and ensure that the entity adheres to the provisions of the ISE Privacy Guidelines and other requirement 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 entity counsel.]

   The [name of entity]'s privacy committee is guided by a trained Privacy Officer [who is the (position) of the entity and] who is appointed by the Director of the entity. The Privacy Officer receives reports regarding alleged errors and violations of the provisions of this policy, receives and coordinates complaint resolution under the entity'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?**

   The [name of entity]'s Privacy Officer ensures that enforcement procedures and sanctions outlined in [insert section number of policy (see Section N.3, Enforcement)] are adequate and enforced.

D. Definitions

1. **What key words or phrases are regularly used in the policy for which the entity 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, Glossary of Terms and Definitions.

   For examples of primary terms and definitions used in this policy, refer to [insert section or appendix citation].

E. Information

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

   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, drivers' records, identification, and commercial databases.

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

   The [name of entity] 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 entity 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. **Identify what information *may not* be sought, retained, shared, or disclosed by the entity.**

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

   The [name of entity] will not seek or retain and information-originating entities 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 race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation.

3. **Does your entity apply labels to information (or ensure that the originating entity 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, Glossary of Terms and Definitions.) 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 the retention or disclosure of certain types of information; for example, the identity of a sexual assault victim.**

The [name of entity] applies labels to entity-originated information (or ensures that the originating entity has applied labels) to indicate to the accessing authorized user that:

- The information is "protected information," to include "personal data" on any individual (see Terms and Definitions, within this 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. **Does your entity categorize information (or ensure that the originating entity 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.**

   The [name of entity] 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 entity 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).

5. **When information is gathered or collected and retained by the entity, 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)?**

   At the time a decision is made by the [name of entity] 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?**

   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.

7. If your entity 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 entity 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 entity 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 entities?**
- **Access and dissemination (data retrieval and dissemination)—The process of making the information available to other entities and obtaining feedback on investigative outcomes?**
- **Retention and security of the information?**

Note: Some entities, 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.

The [name of entity] 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 entity 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 (PII).
- Regularly provide access to or disseminate the information in response to an interentity inquiry for law enforcement, homeland security, or public safety and analytical purposes or provide an assessment of the information to any 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 entity'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 entity 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?

The [name of entity] 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 entity 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 entity 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 entity is making available in the ISE, such that participants can handle the information in accordance with applicable legal requirements?

Refer to Appendix A, Glossary of Terms and Definitions, for a definition of metadata.

The [name of entity] will identify and review protected information that may be accessed from or disseminated by the entity prior to sharing that information through the Information Sharing Environment. Further, the entity 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 an entity 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.

10. Does your entity 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 entity, department, component, and subcomponent (when applicable).**
- **If applicable, the name of the entity's justice information system from which the information is disseminated.**
- **The date the information was collected (submitted) and, when 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.**

The [name of entity] 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 entity, department or entity, component, and subcomponent.
- The name of the entity's justice information system from which the information is disseminated.
- The date the information was collected and, when 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 entity 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?

The [name of entity] 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 entity maintain a record of the source of the information sought and collected?

The [name of entity] will keep a record of the source of all information sought and collected by the entity.

F. Acquiring and Receiving Information

1. Are there applicable state and federal constitutional provisions and statutes that govern or specify the techniques and methods the entity may employ when seeking and receiving information?

Identify and list laws and provisions in the policy. Refer to Appendix B for synopses of primary federal laws relevant to seeking, retaining, or disseminating justice information.

Information-gathering (acquisition) and access and investigative techniques used by the [name of entity] and information-originating entities 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 entity policy).
- Criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) *National Criminal Intelligence Sharing Plan* (NCISP).
- Constitutional provisions; statute, Section [insert number]; and administrative rules, as well as regulations and policies that apply to multijurisdictional intelligence and information databases.

2. Does your entity'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 entity and participating entity staff trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism?

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

3. Does your entity'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?

The [name of entity]'s SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals and/or organizations involved in activities that have been determined to be consistent with criminal activities associated with terrorism will be documented and shared through the ISE. These safeguards are intended to ensure that information which 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.

4. Does the entity (if operational, conducting investigations) adhere to a policy regarding the investigative techniques the entity will follow when acquiring information (for example, an intrusion-level statement)?

Information-gathering and investigative techniques used by the [name of entity] will and those used by originating agencies should be the least intrusive means necessary in the particular circumstances to gather information the entity is authorized to seek or retain.

5. **Do agencies that access your entity's information and/or share information with your entity ensure that they will adhere to applicable laws and policies?**

   External agencies that access the [name of entity]'s information or share information with the entity will provide an assurance (i.e., within interagency agreements, MOUs, etc.) that they comply with laws and rules governing those individual entities, including applicable federal and state laws.

6. **If the entity contracts with commercial databases, how does the entity ensure that the commercial database company is in legal compliance in its information-gathering techniques?**

   The [name of entity] will contract only with commercial database companies that provide an assurance that their methods for gathering PII 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 agencies or institutions or classes of individuals) from which the entity will not receive, seek, accept, or retain information?**

   The [name of entity] will not directly or indirectly receive, seek, accept, or retain information from:

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

G. Information Quality Assurance

1. **Does your entity have established protocols and procedures (manual and electronic) to ensure the quality (for example, accurate, complete, current, verifiable, and reliable) of the information it collects, maintains, and disseminates?**

   The [name of entity] 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 entity 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)?**

   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 entity research alleged or suspected errors and deficiencies (or refer them to the originating agency)? How does your entity respond to confirmed errors or deficiencies?**

   The [name of entity] 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 entity 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?**

   The labeling of retained information will be reevaluated by the [name of entity] 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 entity 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 entity's procedure for correction or destruction?**

   The [name of entity] 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 entity identifies information that is erroneous, misleading, obsolete, or otherwise unreliable; the entity did not have authority to gather the information or to provide the information to another agency; or the entity used prohibited means to gather the information (except when the entity's information source did not act as the agent of the entity in gathering the information).

6. **When the entity 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 entity notify the originating agency or the originating agency's Privacy Officer? What method is used to notify the agency (written, telephone, or electronic notification)?**

   Originating agencies external to the [name of entity] are responsible for reviewing the quality and accuracy of the data provided to the entity. The entity 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 entity 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 entity notify the external agency? What method is used to notify the agency (written, telephone, or electronic notification)?**

   The [name of entity] will use written or electronic notification to inform recipient agencies when information previously provided to the recipient agency is deleted or changed by the entity 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

1. **Who is authorized (position/title, credentials, clearance level[s], etc.) to analyze information acquired or accessed by the entity?**

   Information acquired or received by the [name of entity] 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?**

   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?**

   <u>Best Practice</u>: Does the entity's Privacy Officer or privacy oversight committee review (and approve) all analytical products prior to dissemination or sharing by the entity?

   Information acquired or received by the [name of entity] 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 entity.

- 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 entity] 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 entity.

I. Merging Records

1. Who is authorized (position/title, credentials, clearance level[s], etc.) to merge records?

Information will be merged 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 matching criteria does your entity 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?

Example 1:

Records about an individual or organization from two or more sources will not be merged by the [name of entity] unless there is sufficient identifying information to clearly establish 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:

The set of identifying information sufficient to allow merging by the [name of entity] 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.

3. If the criteria specified in Section I.2 are not met, does the entity have a procedure for associating records?

If the matching requirements are not fully met but there is reason to believe the records are about the same individual, the information may be associated by the [name of entity] 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 Dissemination

1. What types of user actions and permissions are controlled by the entity's access limitations?

Note: User actions and permissions are often used to identify entities 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 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 entities specify their method for identifying user actions and permissions in their privacy policies.

Credentialed, role-based access criteria will be used by the [name of entity], 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 entity use a standard reporting format and commonly accepted data collection codes, and does the entity's SAR information sharing process comply with the ISE Functional Standard for suspicious activity reporting?

Refer to Section D, Resource List, within the Introduction to 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.

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

3. Describe the conditions and credentials by which access to and disclosure of records retained by the entity will be provided *within the entity or in other governmental agencies*. Is an audit trail kept of access to and disclosure of information retained by the entity (e.g., dissemination logs, algorithms)?

Refer to N.2, Accountability, for more information on audit logs.

Access to or disclosure of records retained by the [name of entity] will be provided only ***to persons within the entity 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 entity for which the person is working. An audit trail sufficient to allow the identification of each individual who accessed information retained by the entity and the nature of the information accessed will be kept by the entity.

4. Are participating agencies that access information from your entity 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?

Agencies external to the [name of entity] may not disseminate information accessed or disseminated from the entity without approval from the entity or other originator of the information.

5. Describe the conditions under which access to and disclosure of records retained by the entity 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 entity (e.g., dissemination logs, algorithms)?

Refer to N.2, Accountability, for more information on audit logs.

Records retained by the [name of entity] 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 entity and the nature of the information accessed will be kept by the entity.

6. **Under what circumstances and what legal authority [cite] 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 entity's redress policy? Is an audit trail kept of disclosure of information retained by the entity without the audit trail constituting an impermissible collection of information of a member of the public (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 an entity chooses to provide nonsensitive information to the public or to provide sensitive information in accordance with entity policy in response to an emergency situation.

   Information gathered or collected and records retained by the [name of entity] may be accessed or disclosed ***to a member of the public*** only if the information is defined by law [cite applicable law] to be a public record or otherwise appropriate for release to further the entity'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 entity 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 entity and the nature of the information accessed will be kept by the entity but may be disclosed only in connection to a challenge to the legitimacy of the disclosure itself but not for investigatory or other criminal justice purposes.

7. **If release of information can be made only under specific conditions (for specific purposes or to specific persons), are those conditions described? Is an audit trail kept showing how those conditions were met?**

   Refer to N.2, Accountability, for more information on audit logs.

   Information gathered or collected and records retained by the [name of entity] 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 entity; 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 entity.

8. **Under what circumstances and to whom will the entity *not disclose* records and information?**

   Information gathered or collected and records retained by the [name of entity] ***will not*** be:

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

9. **What are the categories of records that will ordinarily *not be provided* to the public pursuant to applicable legal authority [the policy must cite applicable legal authority for each state category]?**

   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, and in accordance with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010.
   - Investigatory records of law enforcement entities 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 entity that cannot, under [cite applicable law], be shared without permission.
- A violation of an authorized nondisclosure agreement under [cite applicable law].

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

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

K. Redress

K.1 Disclosure

1. If required by state statute, what are the conditions under which the entity 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.

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 entity]. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information (correction). The entity'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. What are the conditions under which the entity will not disclose information to an individual about whom information has been gathered? Does the entity refer the individual to the agency originating the information?

The existence, content, and source of the information will not be made available by the [name of entity] 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 entity.
- The entity 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 entity, the requestor will be referred to the originating agency, if appropriate or required, or the entity will notify the source agency of the request and its determination that disclosure **by the entity** or referral **of the requestor** to the source agency was neither required nor appropriate under applicable law.

K.2 Corrections

1. What is the entity's procedure for handling individuals' requests for correction involving *information the entity has disclosed and can change because it originated the information*? Is a record kept of requests for corrections?

If an individual requests correction of information ***originating with the [name of entity]*** that has been disclosed, the entity'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 entity's procedure for appeal?

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 entity] or the originating agency. The individual will also be informed of the procedure for appeal when the entity 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 entity's process for handling individuals' complaints and objections with regard to information received, maintained, disclosed, or disseminated by the entity? Is the entity'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: Entities are encouraged to make the complaint procedure applicable to all information and intelligence held by the entity 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).

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 entity] and
    (2) Allegedly has resulted in demonstrable harm to the complainant,

The entity will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the entity'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 by law. If the information did not originate with the entity, the Privacy Officer or [insert title of designee or other individual] will notify the originating entity in writing or electronically within 10 days and, upon request, assist such entity to correct any identified data/record deficiencies, purge the information, or verify that the record is accurate. All information held by the entity 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, including incorrectly merged information, or to be out of date. If there is no resolution within 30 days, the entity will not share the information until such time as the complaint has been resolved. A record will be kept by the entity of all complaints and the resulting action taken in response to the complaint.

2. How does the entity determine which complaints involve information that is specifically protected information shared through the ISE?

<u>Note</u>: This question needs to be addressed when an entity does not have a procedure applicable to all protected information under Section K.4, 1.

To delineate protected information shared through the ISE from other data, the [name of entity] maintains records of entities sharing terrorism-related information and employs system mechanisms to identify the originating entity when the information is shared.

L. Security Safeguards

1. **Does your entity 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.

   The [name of entity]'s [insert position title] is designated and trained to serve as the entity's security officer.

2. **What are your entity's physical, procedural, and technical safeguards for ensuring the security of entity data?**

   Describe how the entity 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.

   <u>Best Practice</u>: Reference generally accepted industry or other applicable standard(s) for security with which the entity complies.

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

3. **Does your entity utilize a separate repository system for tips, leads, and SAR information?**

   The [name of entity] 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?**

   The [name of entity] 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 entity personnel authorized to have access to entity information?**

   Access to [name of entity] information will be granted only to entity 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 entity data identify the user?**

   Queries made to the [name of entity]'s data applications will be logged into the data system identifying the user initiating the query.

7. **Is a log kept of accessed and disseminated entity data, and is an audit trail maintained? Refer to N.2, Accountability, for more information on audit logs.**

   The [name of entity] will utilize watch logs to maintain audit trails of requested and disseminated information.

8. **Are risk and vulnerability assessments (if maintained) stored separately from publicly available data?**

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

9. **What are the entity'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 entity has been the subject of a suspected or confirmed data breach.

   Option 1:

   [If there is no applicable state data breach notification law and you choose not to follow the Office of Management and Budget (OMB) guidance in Option 2.] The [name of entity] 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:

   [If there is no applicable state data breach notification law and you choose to follow the OMB guidance.] The [name of entity] 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:

   [If there is an applicable data breach notification law.] The [name of entity] 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 entity] will immediately notify the originating agency from which the entity received personal information of a suspected or confirmed breach of such information.

M. Information Retention and Destruction

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

   Note: A retention and destruction policy should be provided for all information and intelligence databases/records held by the entity.

   All applicable information will be reviewed for record retention (validation or purge) by [name of entity] 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. **Does your entity have a retention and destruction policy? Reference laws, if applicable.**

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

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

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

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.**

   Option 1:

   The procedure contained in [cite law, statute, regulation, or policy] will be followed by [name of entity] 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:

No approval will be required from the originating agency before information held by the [name of entity] 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. Is the source of the information notified prior to removal or destruction?

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

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 entity personnel that a record is due for review and validation or purge)?

A record of information to be reviewed for retention will be maintained by the [name of entity], 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.

7. Is a confirmation of the deletion required?

A printed or electronic confirmation of the deletion will be provided to the originating agency when required under law or if part of the terms of a preestablished agreement with the agency.

N. Accountability and Enforcement

N.1 Information System Transparency

1. Is your entity's privacy policy available to the public?

The [name of entity] will be open with the public in regard to information and intelligence collection practices. The entity's privacy policy will be provided to the public for review, made available upon request, and posted on the entity's Web site [or Web page] at **[insert Web address]**.

2. Does your entity have a point of contact for handling inquiries or complaints?

The [name of entity]'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 entity. 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 entity's data identify the user? Is the identity of the user retained in the audit log?

The audit log of queries made to the [name of entity] will identify the user initiating the query.

2. Is a log kept of accessed and disseminated entity-held data, and is an audit trail maintained?

The [name of entity] 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/entity 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 entity follow to enable evaluation of user compliance with system requirements, the entity's privacy policy, and applicable law?

The [name of entity] 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 entity.

4. **Does your entity have a mechanism for personnel to report errors and violations suspected or confirmed of entity policies related to protected information?**

   The [name of entity]'s personnel or other authorized users shall report errors and suspected or confirmed violations of entity policies relating to protected information to the entity's Privacy Officer. [Cross-reference to policy (see Section C.3).]

5. **Are audits completed by an independent third party or a designated representative of the entity? Are the audits conducted both annually and randomly?**

   The [name of entity] 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 entity'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 entity. The audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the entity's information and intelligence system(s).

6. **How often do you review and update the provisions contained within this privacy policy (for example, annually)?**

   The [name of entity]'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.3 Enforcement

1. **What are your procedures for enforcement if entity 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?**

   If entity 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 entity Director] of the [name of entity] will:

   - Suspend or discontinue access to information by the entity personnel, the participating agency, or the authorized user.
   - Suspend, demote, transfer, or terminate entity personnel, as permitted by applicable personnel policies.
   - Apply administrative actions or sanctions as provided by [state entity or agency] rules and regulations or as provided in entity/agency personnel policies.
   - If the authorized user is from an agency external to the entity, request that the user's employer initiate disciplinary proceedings to enforce the policy's provisions.
   - Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

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

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

O. Training

1. What personnel does your entity require to participate in training programs regarding implementation of and adherence to this privacy policy?

The [name of entity] 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 entity.
- Personnel providing information technology services to the entity.
- Staff in other public agencies or private contractors providing services to the entity.
- Users who are not employed by the entity or a contractor.

2. Do you provide training to personnel authorized to share protected information through the ISE?

The [name of entity] will provide special training regarding the entity'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)?

The [name of entity]'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 entity.
- 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 potential impact of violations of the entity's privacy policy.
- Mechanisms for reporting violations of entity 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—Glossary of Terms and Definitions

The following is a list of primary terms and definitions used throughout this template. These terms are also useful in drafting the definitions section of the entity'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—A participating agency that accesses, contributes, and/or shares information in the [name of entity]'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 entity] and all participating state entities of the [name of entity].

Civil Liberties—According to the U.S. Department of Justice's Global Justice Information Sharing Initiative, the term "civil liberties" refers to 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.

Civil Rights—The term "civil rights" refers to those rights and privileges of citizenship and equal protection that the state is constitutionally bound to guarantee all citizens regardless of race, religion, sex, or other characteristics unrelated to the worth of the individual. Protection of civil rights imposes an affirmative obligation upon government to promote equal protection under the law. These civil rights to personal liberty are guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments and by acts of Congress. Generally, the term "civil rights" involves positive (or affirmative) government action to protect against infringement, while the term "civil liberties" involves restrictions on government.[1]

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 are 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 entity 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, entity, or organization outside the entity 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

1 Civil Rights and Civil Liberties Protections Guidance (September 2008). The definition of civil rights is a modified version of the definition contained in the *National Criminal Intelligence Sharing Plan* (NCISP), at pp. 5–6.

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.

Entity—The [name of entity] that is the subject and owner of the privacy policy.

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. This may be information that is maintained in a records management system, a 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 entity 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 entities 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 (IQ)—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 IQ have been identified as accuracy, completeness, currency, reliability, and context/meaning. Today, IQ 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 entity effectiveness toward reducing crimes, protecting community assets, and preparing for responses. ILP provides law enforcement entities 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 entities.

Law Enforcement Information—For purposes of the ISE, law enforcement information means any information obtained by or of interest to a law enforcement entity 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 counterterrorism 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 Entity—The entity or organizational entity that documents information or data, including source entities that document SAR (and, when authorized, ISE-SAR) information that is collected by an entity.

Participating Entity—An organizational entity that is authorized to access or receive and use entity 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, a directory, or a printer. Permissions must be granted by the system administrator to individual user accounts or administrative groups.

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

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 (PII).

Personally Identifiable Information (PII)—PII is one or more pieces of information that, when considered alone or in the context of how the information is presented or gathered, can contribute to specify (identify) a unique individual. The pieces of information can be personal data, such as biometric characteristics or a unique set of numbers or characters assigned to a specific individual; behavioral data, such as locations or activities; or communications such as innermost thoughts and feelings. Information is personally identifiable even if it carries no explicit and immediately apparent indication of the individual to whom it belongs and even if identification of

a unique individual is not contemplated at the time the information is collected or in the use to which it is put. For example, personally identifiable information includes pictures of a crowd at a public event, even though no one is yet identified and no one may ever be identified, but it does not include the weather at the event. The fact that the event occurred, if not public information, may also be personally identifiable information since, if put together with an attendance list, it constitutes personally identifiable information about behavior.

Persons—Executive Order 12333 defines "United States persons" as United States citizens, aliens known by the intelligence entity 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 entities, "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 entity will adhere to those legal requirements and entity 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 entity, 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—Protected information includes personal data about individuals that is subject to information privacy or other legal protections by law, including the U.S. Constitution and the [insert name of state] Constitution; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 12; applicable state and tribal constitutions; and applicable state, local, and tribal laws and ordinances. Protection may also be extended to organizations by center policy or state, local, or tribal law.

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 entity'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 entity or participating entity.

Public does not include:

- Any employees of the entity or participating entity.
- People or entities, private or governmental, who assist the entity in the operation of the justice information system.
- Public entities whose authority to access information gathered and retained by the entity 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 PII and is maintained, collected, used, or disseminated by or for the collecting entity or organization.

Redress—Laws, policies, and procedures that address public entity 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 entity'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 entity 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 Entity—Source entity refers to the entity 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 entity and, if applicable, a state or regional entity. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor is it designed to support interentity 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 information or reports generated from inside or outside a law enforcement entity that alleges or indicates 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.

U.S. Persons—Refer to Persons.

User—Entity employee or an individual representing a participating entity who is authorized to access or receive and use an entity's information and intelligence databases and resources for lawful purposes.

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

The U.S. Constitution is known as the primary authority that applies to federal as well as state, local, and tribal (SLT) entities. 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 entities'/agencies' privacy policies. While SLT entities 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 entity (e.g., a memorandum of agreement or memorandum of understanding). When relevant or possibly relevant, entities/agencies are advised to list laws, regulations, and policies within their privacy policy, 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 agency personnel and authorized users to ensure that they are aware of the legal and privacy framework within which they and the agency must operate. If the applicability and requirements of various laws, regulations, or sharing agreements are not spelled out or referenced in an entity 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 entity 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 are synopses of primary federal laws that an agency should review and, when appropriate, cite within the policy when developing a privacy policy for a justice information system. The list is arranged in alphabetical order by popular name.

1. **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**—The Brady Act, passed in 1993, requires background checks for purchases of firearms from federally licensed sellers. Because the act prohibits possession of firearms by persons with certain criminal or immigration histories, the transmission of personal data is an integral part of the regulation.

2. **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 (OMB), Memorandum M-01-05, "Guidance on Interagency Sharing of Personal Data– Protecting Personal Privacy," December 20, 2000**—The Computer Matching and Privacy Act of 1988 (Matching Act) amended the Privacy Act of 1974 to require that data-matching activities or programs of federal agencies that are designed to establish or verify eligibility for federal benefit programs or for recouping payments for debts under covered programs protect personal information. This is accomplished through a computer matching agreement and publication of a notice in the *Federal Register*. The OMB guidance requires that interagency data sharing provide protection, including provisions for notice, consent (as appropriate), redisclosure limitations, accuracy, security controls, minimization, accountability, and use of Privacy Impact Assessments. Although not directly a requirement of state, local, and tribal (SLT) agencies, the guidance is a useful source of information on the types of protections that should be considered for all interagency data sharing programs.

3. **Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFR Part 2, Code of Federal Regulations, Title 42: Public Health, Part 2**—42 CFR Part 2 establishes minimum standards to govern the sharing of substance abuse treatment records (patient history information) in programs that are federally assisted. Generally, the sharing of such information is limited to the minimum necessary for the allowed purpose and requires consent of the patient except in specific emergency situations, pursuant to a court order or as otherwise specified. State law should also be consulted to determine whether there are additional limitations or sharing requirements.

4. **Confidentiality of Identifiable Research and Statistical Information, 28 CFR Part 22, Code of Federal Regulations, Title 28, Chapter I, Part 22**—28 CFR Part 22 is designed to protect the privacy of individuals whose personal information is made available for use in a research or statistical program funded under the Omnibus Crime Control and Safe Streets Act of 1968, the Juvenile Justice and Delinquency Prevention Act of 1974, or the Victim of Crimes Act. The regulation, which may apply to SLT agencies that conduct research or statistical programs, limits the use of such information to research or statistical purposes; limits its revelation to a need-to-know basis; provides for final disposition, transfer, and notice to/consent of data subjects; and identifies sanctions for violations. It provides useful guidance for SLT agencies that wish to make data containing personal information available for research or statistical purposes.

5. **Crime Identification Technology, 42 U.S.C. § 14601, United States Code, Title 42, Chapter 140, Subchapter I, § 14601**—This statute authorizes the Office of Justice Programs (OJP), U.S. Department of Justice (DOJ), to support technological advances by states directed at a variety of criminal justice purposes, such as identification of certain categories of offenders, conducting background checks, and determining eligibility for firearms possession. The act defines broad categories of purposes for which funds may be used by OJP and sets forth certain eligibility criteria and assurances and other protocols that must be followed.

6. **Criminal History Records Exchanged for Noncriminal Justice Purposes, 42 U.S.C. § 14611, United States Code, Title 42, Chapter 140, Subchapter II, § 14611**—This statute provides a general overview of the Interstate Identification Index System (IIIS), an information sharing system that contains state and federal criminal history records that are also used for non-criminal justice purposes, such as governmental licensing and employment background checks. Congress recommends the creation of interstate and federal-state agreements to ensure that uniform policies are in place for records exchanges for non-criminal justice purposes and to prevent unauthorized

use and disclosure of personal information due to variances in authorized users' policies. This statute is applicable to multijurisdictional information sharing systems that allow non-criminal justice-related exchanges.

7. **Criminal Intelligence Systems Operating Policies, 28 CFR Part 23, Code of Federal Regulations, Title 28, Chapter 1, Part 23**—This is a guideline for law enforcement agencies that operate federally funded multijurisdictional criminal intelligence systems. The operating principles of 28 CFR Part 23 provide guidance to law enforcement regarding how to operate criminal intelligence information systems effectively while safeguarding privacy, civil rights, and civil liberties during the collection, storage, and dissemination of criminal intelligence information. The regulation governs the intelligence information systems' process, which includes information submission or collection, secure storage, inquiry and search capability, controlled dissemination, and review and purge processes.

8. **Criminal Justice Information Systems, 28 CFR Part 20, Code of Federal Regulations, Title 28, Chapter 1, Part 20**—This applies to all state and local agencies and individuals collecting, storing, or disseminating criminal history record information processed by manual or automated operations and funded by the Law Enforcement Assistance Administration subsequent to July 1, 1973. The regulation requires those criminal justice information systems to submit a criminal history information plan and provides guidance on specific areas that should have a set of operational procedures. These areas include completeness and accuracy of criminal history records and limitations on dissemination, including general policies on use and dissemination, juvenile records, audits, security, and access and review.

9. **Disposal of Consumer Report Information and Records, 16 CFR Part 682, Code of Federal Regulations, Title 16, Chapter I, Part 682**—16 CFR Part 682 applies to information systems that maintain or possess consumer information for business purposes. The regulation provides guidance on proper disposal procedures for consumer information records to help protect against unauthorized use or access.

10. **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**—This set of statutes prohibits a person from intentionally intercepting, trying to intercept, or asking another person to intercept or try to intercept any wire, oral, or electronic communication or trying to use information obtained in this manner. From another perspective, the law describes what law enforcement may do to intercept communications and how an organization may draft its acceptable use policies and monitor communications. Although it is a federal statute, the act does apply to state and local agencies and officials.

11. **Fair Credit Reporting Act, 15 U.S.C. § 1681, United States Code, Title 15, Chapter 41, Subchapter III, § 1681**—The Fair Credit Reporting Act regulates the collection, dissemination, and use of consumer information, including consumer credit information by consumer reporting agencies. Consumer reporting agencies include specialty agencies, such as agencies that sell information about employment history, insurance claims, check-writing histories, medical records, and rental history records, as well as credit bureaus. The law primarily deals with the rights of people about whom information has been gathered by consumer reporting agencies and the obligations of the agencies. Government agencies may obtain information from these reporting agencies and should be aware of the nature and limitations of the information, in terms of collection, retention, and error correction.

12. **Federal Civil Rights laws, 42 U.S.C. § 1983, United States Code, Title 42, Chapter 21, Subchapter I, § 1983**—This is a federal statute that allows an individual to sue public officials in federal court for violations of the individual's civil rights. Civil rights include such things as the Fourth Amendment's prohibitions against unreasonable search and seizure, violations of privacy rights, and violations of the right to freedom of religion, free speech, and free association. It serves as a deterrent to unlawful collection, use, or sharing of information rather than providing specific authority or a prohibition to the collection, use, or sharing of information.

13. **Federal Records Act, 44 U.S.C. § 3301, United States Code, Title 44, Chapter 33, § 3301**—This chapter contains the laws governing disposal of records made or received by a federal agency in the normal course of business. It discusses destruction procedures and notices, if required, and the role of the federal archivist. The law applies only to federal agencies, but there may be similar state or local laws applicable to state and local agencies.

14. **Freedom of Information Act (FOIA), 5 U.S.C. § 552, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552**—The federal FOIA, enacted in 1966, provides access to federal agency records or information. It does not, however, allow access to state or local government records. Nearly all states have their own public access statutes that provide access to state- and local-agency records. The interaction of federal and state FOIA laws can create complex issues. Federal statutes, in essence, provide a baseline of legal protections for individuals. While state legislatures may pass laws to supplement these federal guidelines, state laws that interfere with or are contrary to a federal law are preempted. By virtue of the Supremacy Clause of the U.S. Constitution (Article VI, Clause 2), federal law may restrict access to records otherwise available pursuant to a state's FOIA by requiring that certain information be kept confidential. Thus, federal confidentiality requirements may supersede a state FOIA statute mandating public disclosure of a record, but only when there is a specific federal statute (other than the federal FOIA) that mandates the records be kept confidential. In short, records may be available under one FOIA statute but not pursuant to another.

15. **Health Insurance Portability and Accountability Act (HIPAA) of 1996, 42 U.S.C. § 201, United States Code, Title 42, Chapter 6A, Subchapter I, § 201; Public Law 104-191**—HIPAA was enacted to improve the Medicare and Medicaid programs and the efficiency and effectiveness of the nation's health care system by encouraging the development of a national health information system through the establishment of standards and requirements for the electronic transmission of health information. To that end, Congress directed the U.S. Department of Health and Human Services (HHS) to issue safeguards to protect the security and confidentiality of health information. To implement HIPAA's privacy requirements, HHS promulgated regulations setting national privacy standards for health information: the Standards for Privacy of Individually Identifiable Health Information (the "Privacy Rule")—42 U.S.C. §1320d-2; 45 CFR Parts 160, 164 (2003).

16. **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**—This "Privacy Rule" sets forth national standards for the privacy and security of individually identifiable health information (45 CFR Part 164, Subpart E (2003)). This rule has been described as providing a "federal floor" of safeguards to protect the confidentiality of medical information. State laws that provide stronger privacy protection will continue to apply over and above the federal privacy protection. The general rule under these standards states that a covered entity may not use or disclose protected health information except as permitted or required by the rules (45 CFR Part 164.502(a) and §164.103 [defining protected health information and use]). The Privacy Rule applies to the following covered entities: (1) a health plan, (2) a health care clearinghouse, and (3) a health care provider who transmits any health information in electronic form in connection with certain transactions (42 U.S.C. §1320d-1(a) (2003); 45 CFR Part 160.102 (2003)). Since the Privacy Rule applies only to a covered entity, a governmental body begins its inquiry by first determining whether it is a covered entity under the Privacy Rule (45 CFR Part 160.103 (2003) [defining health plan, health care clearinghouse, health care provider]). If it is a covered entity, it then looks to the Privacy Rule for a permitted or required disclosure.

17. **Indian Civil Rights Act of 1968, 25 U.S.C. § 1301 et seq., United States Code, Title 25, Chapter 15, Subchapter I**—This act contains definitions of relevant terms and extends certain constitutional rights to Indian tribes exercising powers of self-government.

18. **Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Section 1016, as amended by the 9/11 Commission Act**—This act broadly affects U.S. terrorism law and applies directly to the federal government. It establishes the Director of National Intelligence, the National Counterterrorism Center, and the Privacy and Civil Liberties Oversight Board. Of importance to SLT agencies, IRTPA establishes the Information Sharing Environment (ISE) (see Appendix A, Glossary of Terms and Definitions) for the sharing of terrorism-related information at all levels of government, with private agencies, and with foreign partners.

19. **National Child Protection Act of 1993, Public Law 103-209 (December 20, 1993), 107 Stat. 2490**—In each state, an authorized criminal justice agency of the state shall report child abuse crime information to or index child abuse crime information in the national criminal history background check system. A criminal justice agency can satisfy the requirement by reporting or indexing all felony and serious misdemeanor arrests and dispositions. The U.S. Attorney General (AG) is required to publish an annual statistical summary of child abuse crimes. The act requires that 80 percent of final dispositions be

entered in the state databases by December 1998, with steps being taken toward 100 percent entry.

A 1994 amendment required that the AG—in consultation with federal, state, and local officials, including officials responsible for criminal history record systems, and representatives of public and private care organizations and health, legal, and social welfare organizations—shall develop guidelines for the adoption of appropriate safeguards by care providers and by the state for protecting children, the elderly, and individuals with disabilities from abuse.

20. **National Crime Prevention and Privacy Compact, 42 U.S.C. § 14616, United States Code, Title 42, Chapter 140, Subchapter II, § 14616**—The compact establishes an infrastructure by which states can exchange criminal records for non-criminal justice purposes according to the laws of the requesting state and provide reciprocity among the states to share records without charging each other for the information. The Compact Council, as a national independent authority, works in partnership with criminal history record custodians, end users, and policymakers to regulate and facilitate the sharing of complete, accurate, and timely criminal history record information to non-criminal justice users in order to enhance public safety, welfare, and the security of society while recognizing the importance of individual privacy rights.

21. **National Security Act, Public Law 235, Section 606, in accordance with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010**—The National Security Act of 1947 mandated a major reorganization of foreign policy and military establishments of the U.S. government. The act created many of the institutions that U.S. Presidents found useful when formulating and implementing foreign policy, including the National Security Council and the Central Intelligence Agency. The 1947 law also caused far-reaching changes in the military establishment. The War Department and Navy Department merged into a single U.S. Department of Defense under the Secretary of Defense, who also directed the newly created Department of the Air Force. However, each of the three branches maintained their own service secretaries.

    On October 7, 2011, President Barack Obama signed Executive Order 13549, entitled, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information." This order directs structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks that shall be consistent with appropriate protections for privacy and civil liberties. Agencies bear the primary responsibility for meeting these twin goals. These structural reforms will ensure coordinated interagency development and reliable implementation of policies and minimum standards regarding information security, personnel security, and systems security; address both internal and external security threats and vulnerabilities; and provide policies and minimum standards for sharing classified information both within and outside the federal government. These policies and minimum standards will address all agencies that operate or access classified computer networks, all users of classified computer networks (including contractors and others who operate or access classified computer networks controlled by the federal government), and all classified information on those networks.

22. **Privacy Act of 1974, 5 U.S.C. § 552a, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a**—This section of the Privacy Act prohibits the release of records from a record system without the expressed consent of the individual to whom the record pertains. This provision does not apply to court orders for records or when a written request is made by the head of a government agency tasked with civil or criminal law. Additionally, the head of any agency can promulgate rules to exempt a system of records if it is maintained by an agency whose principal function is to enforce criminal laws and if the information is compiled for the purpose of a criminal identification, investigation, or any other stage of the criminal process.

23. **Privacy of Consumer Financial Information, 16 CFR Part 313, Code of Federal Regulations, Title 16, Chapter I, Part 313**—This code oversees the treatment of nonpublic personal information about consumers by financial institutions and requires the institution to provide notice to customers about its privacy policies, the conditions under which it can disclose this information, and its opt-out policies. This code also prohibits the disclosure of a consumer's credit card, deposit, or transaction account information to nonaffiliated third parties to market to the customer. The requirements for initial notice for the "opt-out" do not apply when nonpublic personal information is disclosed in order to comply with federal, state, or local laws or to comply with an authorized investigation, subpoena, or summons.

24. **Protection of Sensitive Agency Information, Office of Management and Budget Memorandum M-06-16 (June 2006)**—This memorandum provides a security checklist from the National Institute of Standards and Technology (NIST) to protect remote information removed from or accessed from outside an agency's physical location specific to personally identifiable information (PII). The NIST checklist requires that agencies verify PII in need of protection, confirm the adequacy of organization policy surrounding PII protection, and implement any necessary protections for PII transported or stored off-site or accessed remotely. In addition to the NIST checklist, the memorandum recommends implementing data encryption on all mobile devices, allowing remote access only with two-factor authentication, using timeout functions on devices, and logging all computer-readable data extracts from databases with sensitive information, while verifying each extract has either been erased within 90 days or its use is still required.

25. **Safeguarding Against and Responding to the Breach of Personally Identifiable Information, OMB Memorandum M-07-16 (May 2007)**—This memorandum applies to federal agency-held information and information systems, requiring development and implementation of a breach notification policy applicable to personally identifiable information in the possession of the agency. Development of a breach notification policy includes a review of existing privacy and security requirements, development of requirements for incident reporting and handling, and procedures for internal and external notification. SLT agencies that are not subject to an existing breach notification law or policy may use the federal requirements as a template for developing their own breach notification policy.

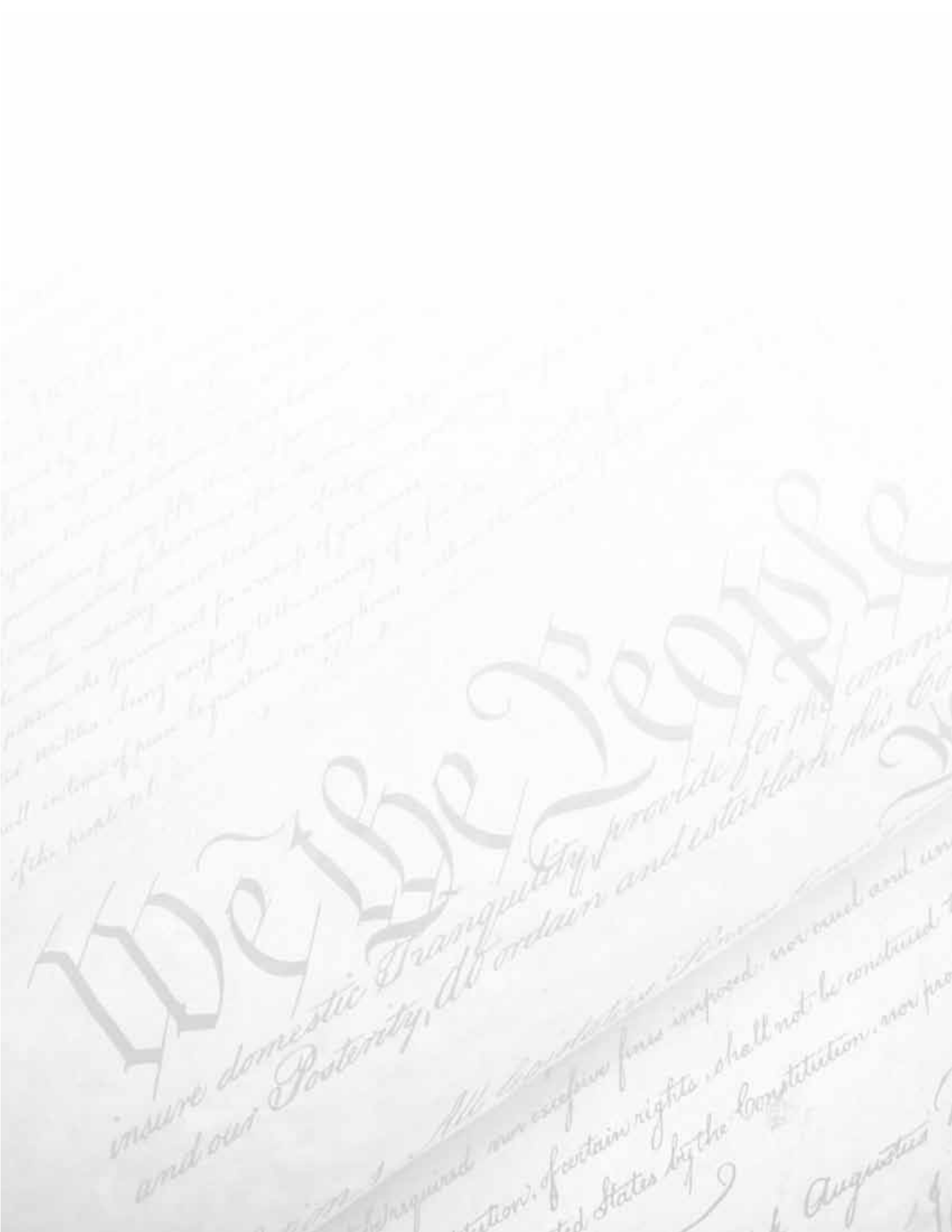
26. **Safeguarding Customer Information, 16 CFR Part 314, Code of Federal Regulations, Title 16, Chapter I, Part 314**—This Federal Trade Commission regulation implements Sections 501 and 505(b)(2) of the Gramm-Leach-Bliley Act. It sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information by financial institutions. While not directly applicable to government agencies, the regulation is useful in outlining the elements of a comprehensive information security program, including administrative, technical, and physical safeguards designed to (1) ensure the security and confidentiality of information, (2) protect against any anticipated threats or hazards to the security or integrity of information, and (3) protect against unauthorized access to or use of information that could result in substantial harm or inconvenience to any individual.

27. **Sarbanes-Oxley Act of 2002, 15 U.S.C., Chapter 98, § 7201, United States Code, Title 15, Chapter 98, § 7201**—The Sarbanes-Oxley Act of 2002, Pub. L. 107-204 (July 30, 2002), commonly called Sarbanes-Oxley, is a federal law that sets new or enhanced standards for all U.S. public company boards, management, and public accounting firms. Its 11 titles include standards for public audits, internal controls, and financial disclosure. While not applicable to federal or state, local, or tribal governmental agencies, the business standards established by Sarbanes-Oxley are of value to such agencies in establishing their own policies and procedures to guide and control their business processes.

28. **U.S. Constitution, First, Fourth, and Sixth Amendments**—The First, Fourth, and Sixth Amendments to the U.S. Constitution and, indeed, the entire Bill of Rights establish minimum standards for the protection of the civil rights and civil liberties of Americans. The First Amendment protects religious freedom, speech, the press, the right to peaceably assemble, and the right to petition the government for a redress of grievances. The Fourth Amendment protects the people from unreasonable searches and seizures and requires that warrants be issued only upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the person or things to be seized. The Sixth Amendment establishes the right of an accused individual to a speedy and public trial by an impartial jury, to be informed of the nature and cause of the charges, to confront witnesses, to have compulsory process to obtain witnesses, and to have the assistance of legal counsel.

29. **USA PATRIOT Act, Public Law 107-56 (October 26, 2001), 115 Stat. 272**—The USA PATRIOT Act was enacted in response to the terrorist attacks of September 11, 2001. The act was designed to reduce the restrictions on law enforcement agencies' ability to gather intelligence and investigate terrorism within the United States, expand the Secretary of the Treasury's authority to regulate financial transactions, particularly those involving foreign individuals and entities, and broaden the discretion of law enforcement and immigration authorities in detaining and deporting illegal immigrants suspected of terrorism-related acts. The act also expanded the definition of "terrorism" to include domestic terrorism, thus enlarging the number of activities to which the USA

PATRIOT Act's law enforcement powers can be applied. In 2011, the act was extended for four years, including provisions for roving wiretaps, searches of business records, and the conduct of surveillance of "lone wolves"—individuals suspected of terrorism-related activities that are not linked to terrorist groups.



Printed 04/12