



United States
Department of Justice

Privacy, Civil Rights, and Civil Liberties Policy Development Guide

For State, Local,
and Tribal Justice Entities

April 2012



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

Where to Locate These Resources

The Global Privacy Resources featured within this guide and others are available online at www.it.ojp.gov/privacy. To request printed copies, 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 overview 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.

4.7.1	When to Perform a PIA?	17
4.7.2	PIA Template.....	17
4.8	Resources	17
4.8.1	Privacy Resources.....	17
4.8.2	Information Quality Resources	18
4.8.3	Security Resources	19
Section 5	Assembling the Project Team	21
5.1	Identifying the Project Champion or Sponsor	21
5.2	Securing Support and Justifying Resources.....	22
5.2.1	Securing Agency Head Support	22
5.2.1.1	<i>Executive Summary for Justice Decision Makers: Privacy, Civil Rights, and Civil Liberties Program Development</i>	22
5.2.1.2	<i>7 Steps to a Privacy, Civil Rights, and Civil Liberties Policy</i>	22
5.2.1.3	<i>The Importance of Privacy, Civil Rights, and Civil Liberties Protections in American Law Enforcement and Public Safety: Line Officer Training Video</i>	22
5.2.2	Justifying Resources	23
5.3	Identifying the Project Team Leader	23
5.4	Building the Project Team and Stakeholder Contacts	24
5.4.1	Project Team.....	24
5.4.2	Stakeholder Contacts	24
5.5	Continuing Roles Within the Entity	25
5.5.1	Privacy Officer	25
5.5.2	Security Officer	25
5.6	Resources	26
Section 6	Establishing a Charter	29
6.1	Components of a Charter	29
6.1.1	Vision Statement.....	30
6.1.2	Mission Statement	30
6.1.3	Values Statement.....	30
6.1.4	Goals and Objectives	31
6.1.4.1	Goals	31
6.1.4.2	Objectives.....	31
6.2	Writing the Charter	32
6.3	Resources	32
Section 7	Understanding Information Exchanges	33
7.1	Understanding Information Exchanges	33
7.1.1	Tools to Assist With Understanding the Flow of Information.....	35
7.1.1.1	Criminal Justice System Flowchart	35
7.1.1.2	<i>Justice Information Privacy Guideline</i>	36

7.1.1.3	Justice Information Exchange Model (JIEM).....	36
7.1.1.4	Information Life Cycle	37
7.2	Privacy Impact Assessment (PIA)	37
7.2.1	PIA Template.....	38
7.3	Resources	38
Section 8	Performing the Legal Analysis	39
8.1	Approach to the Legal Analysis	39
8.2	Focusing the Legal Analysis	40
8.2.1	Suggestions for Approaching the Legal Analysis.....	40
8.2.2	Potential Sources of Legal Authority and Limitations	40
8.2.2.1	Federal Laws Relevant to Seeking, Retaining, and Disseminating Justice Information ...	41
8.2.2.2	State, Municipal, Local, and Other Sources	42
8.2.3	Particular Events and Actions	42
8.2.4	Information Related to a Specific Person	43
8.2.5	Information Related to Groups	43
8.3	Performing the Legal Analysis	44
8.3.1	Principles	44
8.3.1.1	Collection of Information	44
8.3.1.2	Information Quality Relative to Collection and Maintenance of Information.....	45
8.3.1.3	Sharing and Dissemination of Information—Public Access	45
8.3.1.4	Provisions Relevant to Individuals’ Access to Information About Themselves.....	46
8.3.1.5	Information and Record Retention and Destruction	46
8.3.1.6	Entity or Project Transparency	47
8.3.1.7	Accountability and Enforcement.....	47
8.3.2	Specific Laws to Examine.....	47
8.4	Identifying Critical Issues and Policy Gaps.....	50
8.4.1	Identifying Team Members’ Privacy Concerns.....	50
8.4.2	Using Legal Research as a Guide.....	50
8.5	Legal Citations Within the Privacy Policy	51
8.6	Resources	51
Section 9	Writing the Privacy Policy	53
9.1	Vision and Scope for the Policy.....	53
9.2	Policy Outline.....	54
9.3	Writing the Policy.....	55
9.3.1	Making the Policy Choices—Filling in the Gaps	55
9.4	Core Policy Concepts.....	55
9.5	Templates to Assist With Drafting the Privacy Policy.....	60
9.5.1	<i>Privacy, Civil Rights, and Civil Liberties Policy Development Template for State, Local, and Tribal Justice Entities</i>	60

9.6	Perform a Policy Evaluation	60
9.6.1	<i>Policy Review Checklist</i>	60
9.7	Vetting the Privacy Policy	60
9.8	Process for Revisions and Amendments.....	61
9.9	Resources	61
Section 10 Implementing the Privacy Policy		63
10.1	Formal Adoption of the Policy.....	63
10.2	Publication	63
10.3	Outreach.....	63
10.3.1	<i>Guidance for Building Communities of Trust</i>	64
10.4	Training Recommendations.....	64
10.4.1	Trainees.....	64
10.4.2	Content	65
10.4.3	Method.....	65
10.4.4	Frequency.....	65
10.4.5	Additional Resources and Training Tools.....	65
10.4.5.1	Privacy Training Resources	65
10.4.6	Acknowledgment	67
10.4.7	How Will You Measure Your Success?.....	67
10.5	Privacy Officer	67
10.6	Monitoring Policy Implementation.....	68
10.6.1	<i>Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise</i>	68
10.7	Ensuring Compliance	68
10.8	Enforcement	69
10.9	Resources	69
Appendix A Privacy Primers		71
Appendix B Criminal Justice System Flowchart.....		79
Appendix C Privacy Policy Drafting Tools		83
C.1	<i>Privacy, Civil Rights, and Civil Liberties Policy Development Template for State, Local, and Tribal Justice Entities</i> (SLT Policy Development Template).....	85
C.2	Glossary of Terms and Definitions	109
C.3	Federal Laws Relevant to Seeking, Retaining, and Disseminating Justice Information.....	117
Appendix D <i>Policy Review Checklist</i>.....		123
Appendix E Sample Privacy Policies		165
E.1	Hawaii Integrated Justice Information Sharing (HIJIS) Program	165
E.2	CONNECT.....	179

Section 1—Acknowledgments



This *Privacy, Civil Rights, and Civil Liberties Policy Development Guide for State, Local, and Tribal Justice Entities* (“Privacy Guide”) was developed through a collaborative effort of the Global Privacy and Information Quality Working Group (GPIQWG) of the U.S. Department of Justice’s (DOJ) Global Justice Information Sharing Initiative (Global).¹ Global serves as a Federal Advisory Committee (FAC) and advises the U.S. Attorney General on justice information sharing and integration initiatives.

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. GPIQWG is one of five Global working groups 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 (PII)² is appropriately collected, used, and disseminated within integrated justice information systems. GPIQWG addresses accuracy and reliability issues involved in entering and updating criminal history records with subsequent events (e.g., prosecution, adjudication). This work includes exploring biometrics technologies and addressing the privacy, civil rights, civil liberties, and information quality issues these technologies present.

In order to formulate a unified and comprehensive approach to privacy, civil rights, civil liberties, and information quality issues, GPIQWG actively coordinates with the other Global working groups.

Included in this guide is an essential tool for use when drafting comprehensive privacy, civil rights, and civil liberties policies, entitled *Privacy, Civil Rights, and Civil Liberties Policy Development Template for State, Local, and Tribal Justice Entities* (“SLT Policy Development Template”), contained in Appendix C.1. The template is relevant to the administration of justice, strategic and tactical operations, and national security responsibilities and is intended to address all types of public safety and public protection risks and threats, whether criminal or from natural disasters.

This guide is a living document that is routinely reviewed and updated in response to changes in applicable law, technology, and the purpose and use of information systems. It is the product of Global and its membership of justice practitioners and industry professionals. To be responsive to current justice information sharing issues, Global working group memberships are dynamic and dependent on the expertise required at any given time. Therefore, a special thank-you is expressed to the following current GPIQWG members for developing and contributing to this version of the Privacy Guide.

¹ www.it.ojp.gov/global.

² PII is discussed in Section 4.1.1 and defined in Appendix C.2, Glossary of Terms and Definitions.

GPIQWG Membership

**The Honorable Anthony Capizzi,
Chair**

Montgomery County, Ohio,
Juvenile Court
Representing National Council of
Juvenile and Family Court Judges
Dayton, Ohio

Phil Stevenson, Ph.D., Vice Chair

Arizona Criminal Justice
Commission
Phoenix, Arizona

Devon B. Adams

Bureau of Justice Statistics,
Office of Justice Programs,
U.S. Department of Justice
Washington, DC

Francis X. Aumand III

Vermont Department of Public
Safety
Waterbury, Vermont

Alan Carlson

Orange County Superior Court
Santa Ana, California

Ayn Crawley

Office for Civil Rights and Civil
Liberties
U.S. Department of Homeland
Security
Washington, DC

Cabell Cropper

National Criminal Justice
Association
Washington, DC

**Colonel Steven F. Cumoletti, GAC
Member**

New York State Police
Albany, New York

Lieutenant Kathleen deGrasse

Illinois State Police
Des Plaines, Illinois

William A. Ford

National Institute of Justice
Washington, DC

Owen Greenspan

SEARCH, The National Consortium
for Justice Information and
Statistics
Sacramento, California

Bob Greeves

Bureau of Justice Assistance,
Office of Justice Programs,
U.S. Department of Justice
Washington, DC

Alissa Huntoon

Bureau of Justice Assistance,
Office of Justice Programs,
U.S. Department of Justice
Washington, DC

**Barbara Hurst, Esquire, GAC
Member**

Rhode Island Office of the Public
Defender
Providence, Rhode Island

Erin Kenneally, Esquire

eLCHEMY, Inc.
La Jolla, California

Thomas MacLellan

National Governors Association
Washington, DC

Michael McDonald

Delaware State Police
Headquarters
Dover, Delaware

Jennifer McNally

Biometric Center of Excellence,
Criminal Justice Information
Services Division, Federal Bureau
of Investigation

**Sheriff Michael Milstead, GAC
Member**

Minnehaha County, South Dakota,
Sheriff's Office
Sioux Falls, South Dakota

Joe Mollner

Boys & Girls Clubs of America
Atlanta, Georgia

Steve Schuetz

National Institute of Justice,
U.S. Department of Justice
Washington, DC

Steve Serrao

Memex U.S. Law Enforcement
Solutions
Sterling, Virginia

Steve Siegel

Denver District Attorney's Office
Denver, Colorado

Cindy Southworth

National Network to End Domestic
Violence Fund
Washington, DC

Martha Steketee

Independent Consultant
New York, New York

Carl Wicklund, GAC Vice Chair

American Probation and Parole
Association
Lexington, Kentucky

Tammy Woodhams

National Criminal Justice
Association
Washington, DC

Section 2—Foreword



Ethical and legal obligations compel every professional in the justice system, when sharing justice information, to protect privacy, civil rights, and civil liberties interests. For this publication, the term “privacy” captures this multilayered concept—a term meant to embrace all privacy interests, whether rooted in civil rights and civil liberties guarantees, custom, or statutory or regulatory provisions. Today’s increased security needs dictate enhanced justice information sharing and also highlight the need to balance privacy protections with justice information access. The ease of digital access to many types of data now makes analysis of privacy obligations a more complex process. Nonetheless, the foundations for privacy policy exist in our current laws and customs. Constitutions, statutes, regulations, policies, procedures, and common-law requirements still control justice entity³ collection and sharing of information. Today’s justice professionals are challenged to articulate clearly the rules that control their information gathering and sharing activities in a manner that translates into system requirements for both system developers and information managers dealing with digital data.

As mentioned in Section 1, Acknowledgments, the U.S. Department of Justice’s (DOJ) Global Justice Information Sharing Initiative (Global) serves as a Federal Advisory Committee (FAC)⁴ and advises the U.S. Attorney General on justice information sharing and integration initiatives. Global was created to support broadscale exchange of pertinent justice and public safety information. It promotes standards-based electronic information exchange to provide the justice community with timely, accurate, complete, and accessible information in a secure and trusted environment. Global is a “group of groups,” representing more than 30 independent organizations, spanning the spectrum of law enforcement, judicial, correctional, and related bodies. Member organizations participate in Global with a shared responsibility and shared belief that, together, they can bring about positive change by making recommendations to and supporting the initiatives of DOJ.

The Global Privacy and Information Quality Working Group (GPIQWG) is a cross-functional, multidisciplinary working group of Global and is composed of private and local, state, tribal, and federal justice entity representatives. The GPIQWG assists governmental and nongovernmental entities and institutions involved in the justice system in ensuring that PII is appropriately collected, maintained, used, and disseminated within evolving integrated justice information systems.

³ The term “**justice entity**” is used throughout the guide, but the authors recognize nonjustice entity and agency users of this guide.

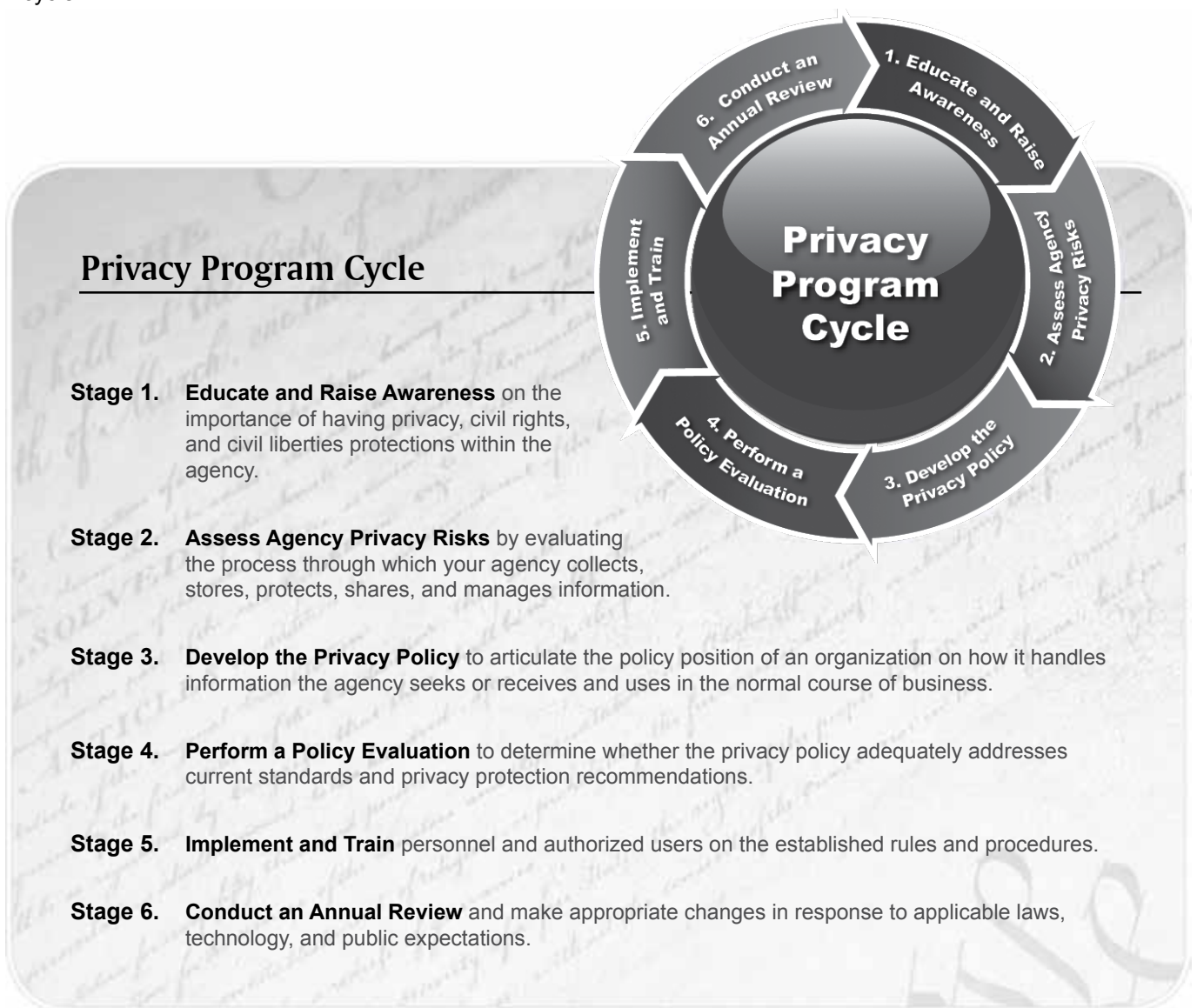
⁴ The Federal Advisory Committee Act, Title 5. Government Organization and Employees, Appendix 2, www.archives.gov/federal-register/laws/fed-advisory-committee/15.html.

The Global privacy vision calls for individual entities to identify their privacy policy requirements within the context of the myriad of legal and societal constraints. Global recognizes the indispensable and primary role of local, state, and tribal justice leadership in enhanced information sharing. Each justice entity must actively define privacy protections and information quality (IQ) requirements for collecting, sharing, and managing the PII that it controls in order to enhance sharing while protecting privacy, civil rights, and civil liberties.

2.1 Global Privacy Resources

To support justice agencies in their efforts to implement privacy, civil rights, and civil liberties policies and protections, GPIQWG, on behalf of Global, published a *Global Privacy Resources*⁵ booklet as a road map to guide justice entities through the diverse privacy policy development and implementation products available today. Each resource featured was developed for state, local, and tribal (SLT) entities by DOJ’s Global or Global partners or through DOJ collaborations with other federal agencies, such as the U.S. Department of Homeland Security (DHS).

Global recognizes that SLT justice entities come in all sizes, with a variety of roles and with varying degrees of available resources. The *Global Privacy Resources* booklet advises entities on what products to use when and for what purpose, through an illustration of these resources according to the stages of an entity privacy program cycle.



⁵ *Global Privacy Resources*, www.it.ojp.gov/privacy.

This Privacy Guide serves as the primary resource for Stage 3: Develop the Privacy Policy, though many of the other resources presented in the booklet are referenced within this guide or contained within its appendices. Some of these are described below. To view all resources featured in the booklet, refer to www.it.ojp.gov/privacy. To request printed copies, send requests to GLOBAL@iir.com.



Executive Summary for Justice Decision Makers: Privacy, Civil Rights, and Civil Liberties Program Development

This executive summary is an awareness resource for justice executives, as well as an informational tool to use for training. The easy-to-read flyer is designed to engender awareness about the topic, make the case for privacy policy development, and underscore the importance of promoting privacy protections within justice agencies. Included is information on basic privacy concepts; the intersection between privacy, security, and information quality; privacy risks; and steps to establish privacy protections through a privacy program cycle. This paper applies settled privacy principles to justice information sharing systems and makes recommendations on best practices.



7 Steps to a Privacy, Civil Rights, and Civil Liberties Policy

Designed for both justice executives and agency personnel, this document raises awareness and educates readers on the seven basic steps involved in the preparation for development of a privacy, civil rights, and civil liberties policy (as recommended in this Privacy Guide). Each step describes the practical tasks associated with preparing for, drafting, and implementing a privacy policy. Also featured is an overview of the core concepts (or chapters) that an agency should address in the written provisions of a privacy policy (as recommended in the SLT Policy Development Template).



Guide to Conducting Privacy Impact Assessments for State, Local, and Tribal Justice Entities

Practitioners are provided a framework with which to examine the privacy implications of their information systems and information sharing collaborations so they can design and implement privacy policies to address vulnerabilities identified through the assessment process. Privacy policies emerge as a result of the analysis performed during the Privacy Impact Assessment (PIA) process. In addition to an overview of the PIA process, this guide contains a template that leads policy developers through a series of appropriate PIA questions that evaluate the process through which personally identifiable information is collected, stored, protected, shared, and managed. The PIA questions are designed to reflect the same policy concepts as those recommended in this Privacy Guide.



Privacy, Civil Rights, and Civil Liberties Policy Development Guide for State, Local, and Tribal Justice Entities (Privacy Guide)

After a Privacy Impact Assessment is completed, the next stage is the development of policies to address privacy, civil rights, and civil liberties vulnerabilities. To assist with this endeavor, GPIQWG developed the *Privacy, Civil Rights, and Civil Liberties Policy Development Guide for State, Local, and Tribal Justice Entities* (this **Privacy Guide**), which includes the resource *Privacy, Civil Rights, and Civil Liberties Policy Development Template for State, Local, and Tribal Justice Entities* (SLT Policy Development Template). These resources are practical hands-on tools for the justice practitioner charged with drafting the privacy policy. They provide sensible guidance for articulating privacy obligations in a manner that protects the justice agency, the individual, and the public. Also included are recommendations on implementation and training.



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

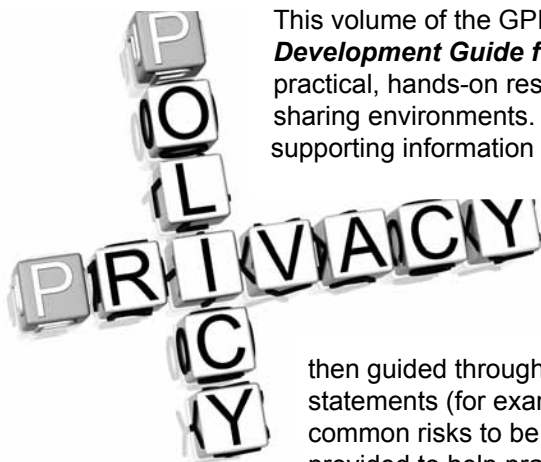
The *Privacy, Civil Rights, and Civil Liberties Policy Development Template for State, Local, and Tribal Justice Entities* (SLT Policy Development Template), contained in Appendix C.1, is provided to assist entity personnel in developing a privacy policy related to the information the entity collects, 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 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, IQ, collation and analysis, merging records, information access and disclosure, redress, security safeguards, retention and destruction, accountability and enforcement, and training. Sample language is included for each provision.



Policy Review Checklist

The checklist is a companion piece to the SLT Policy Development Template and serves both as a self-assessment tool to assist privacy policy authors, project teams, and agency administrators in evaluating whether the provisions contained within their draft policy have met the core concepts recommended in the template, as well as a useful resource for the annual policy review. The checklist is structured according to policy categories and section references that correlate checklist components with those in the template.

Section 3—Introduction



This volume of the GPIQWG privacy series, the ***Privacy, Civil Rights, and Civil Liberties Policy Development Guide for State, Local, and Tribal Justice Entities*** (or “Privacy Guide”), is a practical, hands-on resource that supports analysis of privacy protection requirements for information sharing environments. Its purpose is to guide policy development that protects privacy while supporting information sharing. Basic guidance and information are provided for each step of the policy development process, with resource lists and Web links to more in-depth information on specific subjects.

This guide begins by providing a discussion of privacy and related foundational concepts to provide policy authors with a firm understanding of privacy issues as they relate to information sharing. Readers are

then guided through the planning process, project team development, and drafting of guidance statements (for example, vision, mission, and values statements). The guide identifies certain common risks to be addressed and suggests approaches for issue resolution. Steps are then provided to help practitioners determine what specific information a justice entity collects, uses, and disseminates during the course of routine justice operations and to walk the reader through the identification of laws that control the collection and sharing of that information. With risks, entity information, and applicable laws identified, the guide then instructs policy authors how to develop a privacy, civil rights, and civil liberties privacy policy (utilizing the policy template provided in Appendix C.1) and also provides recommendations for implementation.

It is important to emphasize that a privacy policy is necessary whenever information sharing takes place. In order to provide the appropriate context for each step of the policy development process, it is best to read this guide in its entirety before beginning the process.

The authors of this guide assume the following:

1. The justice entity has, at minimum, a mission statement and, ideally, a strategic plan.
2. There exists (or can be generated) high-level interest and support among the entity’s senior management in developing a privacy policy.
3. There is or will be specifically assigned responsibility for the development, implementation, and auditing (to ensure compliance with) of the privacy policy.

4. An information sharing system includes both the mechanism for sharing information (whether electronic, paper, or verbal) and the governing policies, procedures, and customs.
5. There are probably few, if any, clearly identified resources specifically allocated for privacy policy development.

Section 4—Understanding Foundational Concepts



4.1 What Is Privacy?

This chapter sets out the concepts involved in analyzing privacy issues related to the sharing of information. It discusses privacy and the concept of informational civil liberties and then identifies the privacy ramifications of information sharing. It is important to recognize that the sharing of information does not always implicate privacy interests; therefore, a privacy policy need not be applied to every dissemination of every piece of data. The determination of when there should be adherence to a privacy policy depends on an understanding of what the concept of “privacy” entails. A privacy policy will be relevant when a cognizable privacy interest—as distinguished from a mere “privacy concern”—is involved. Generally, a privacy “concern” is an individual’s subjective desire for secrecy or confidentiality, while a privacy “interest” is an objectively recognized desire that society

deems legitimate and worthy of protection which under certain circumstances may be enforceable in a court or other quasi-judicial system.

In this guide, the term “privacy” is defined as the right of an individual to control how and to what extent information about him or her may be communicated and acted upon.⁶ Privacy interests can be implicated by information about personal behaviors, personal communications, and personal attributes.⁷ In an information sharing context, “privacy” refers to a protected interest of an individual or group in preventing the inappropriate collection, use, maintenance, and disclosure of PII. “Protected” in this context means a legally enforceable (constitutional provision, statute, regulation, or other authoritative order) interest.

Stated differently, privacy interests are not unilateral. They cannot be claimed by an individual without a corresponding recognition in law or custom. As such, “privacy” in the context of information sharing policies concerns information whose confidentiality is enforceable by law or social norms and not merely information backed by a subjective concern. Privacy is rarely, if ever, absolute and may be balanced against countervailing interests of government or other individuals. For example, a person may claim that the fact that he owns property is private and thus insist on excluding that information from being listed on a public municipal Web site. If that concern does not rise to a socially or legally cognizable level or is outweighed by a sufficient governmental activity, it will not constrain information sharing policies.

⁶ Charles Weiss, “The Coming Technology of Knowledge Discovery: A Final Blow to Privacy Protection?” *University of Illinois Journal of Law, Technology and Privacy*, 2004, citing Alan F. Westin, *Privacy and Freedom*, p. 7 (1967).

⁷ Of course, there is also a strong privacy interest in personal thoughts, but government action intruding upon that interest, such as compelled compliance with psychiatric evaluations, is outside this scope because by definition the information resulting from that compulsion can be shared only *after* the initial intrusion is accomplished.

There are many other meanings of “privacy,” both in ordinary parlance and in law and steeped in the corporeal context, as opposed to “information privacy.” In the simplest terms, privacy is commonly accepted as the desire to be left alone.⁸ For example, an individual carries privacy expectations that a family member cannot inspect his diary or an employer should not monitor her after-work activities. Privacy also refers to protected conduct and information in contexts unrelated to information sharing and, therefore, also outside the scope of this policy. For example, privacy is a constitutional concept of individual autonomy and decision making, implicated by activities such as human reproduction and medical decision making. It may protect the right of a high school student to wear his hair long or the right of a patient to refuse a lifesaving operation.

Finally, privacy often refers to a particular collection of laws and principles relevant to a specific context. One example is the Fourth Amendment of the United States Constitution, which prohibits unreasonable searches and seizures by the government. However, with regard to the extent to which the Fourth Amendment protects the principles of privacy, information is protected only when there is a specific legal redress granted to an individual, such as exclusion of evidence or a right to sue for damages. As a result, when those specific remedies are not available, the law will say there has been no Fourth Amendment violation, even though there may well have been an intrusion into protected privacy interests outside the Fourth Amendment. For this reason, informational privacy is more often thought of as a First Amendment issue.

When weighing the contexts (circumstances and conditions) involving the sharing of data, two separate lines of inquiry should be pursued. First, the strength of the particular privacy interest at stake must be evaluated. Is the interest substantial or merely tangential? Is it protected by law, regulation, or custom? Second, because the sharing of information is often integral to conducting business, the impact on the governmental entity proposing to receive or disseminate the data should be considered. Is the sharing of data closely related to a legitimate purpose of the government entity? Is the scope of the sharing as closely tailored as possible to accomplish that purpose? The goal will be to apply the privacy policy in a way that most equitably balances respect for the subject’s privacy interest with the legitimate interests of the governmental entity in sharing the data.

For example, law enforcement often engages in mapping particular crimes, and the public can benefit from that information. Mapping of domestic violence and sexual assault offenses, however, can generate a particular threat to an individual’s privacy since it can be combined with accessible information about residential addresses, publicly broadcasting the location or even the identity of victims of these sensitive crimes. If the privacy interests are understood and appreciated, law enforcement could accommodate its legitimate benefit of mapping with masking techniques that either eliminate or greatly reduce the possibility of identifying specific victims who have an interest in not disclosing this information to the public.

Finally, sharing involves both a provider of information and a recipient. An information privacy policy should address the safeguarding of information by the provider even after it is disseminated. For example, it is often appropriate for information to be shared subject to conditions of use, management, and disclosure that are consistent with the policies or practices of the agency that collected and disseminated the information.

4.1.1 What Is Personally Identifiable Information?

Personally identifiable information (PII) is one or more pieces of information that, when considered alone, in combination with data from other sources, or in the context of how the information is presented or gathered, can contribute to distinguish (identify) an individual. PII can include 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, PII 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, even if not public information, may also be PII since, if put together with an attendance list, it constitutes PII about behavior.

⁸ Dean Prosser, “Privacy,” 48 *California Law Review*, 383, 1960.

Technology continues to amplify the quality, quantity, and meaning of data about individuals, thereby altering the concepts of PII and privacy with consequences for information sharing. The traditional notion of PII reflects the technologically immature, offline environment in which information was created, collected, used, and disclosed. In this corporeal “real space” context, first-order data, such as names, addresses and social security numbers, raise privacy concerns. Technology development, particularly the proliferation of electronic communications networks, has migrated the unit of privacy risk beyond first-order personal identifiers to information that may, on its own, not be personally identifying, but which, when linked together, implicates protectable privacy interests. PII now encompasses information related to a person’s communications, transactions, behaviors, and personal attributes.

It is important to keep in mind that the sharing of PII is often necessary for government agencies carrying out their legitimate and essential work. A good privacy policy attempts to distinguish between information that is needed in order for government to do its job and information that is simply wanted, or is superfluous or redundant. Law enforcement, for example, could not operate without a vibrant exchange of PII. Not all PII is protected, and not all sharing of PII implicates privacy interests. For example, names and addresses in a telephone book are publicly accessible, but the same information in connection with hits on a pornography Web site would implicate significant privacy issues.

4.1.2 Contextual Privacy

Much information is protected, usually by law, because of its nature, such as social security numbers, financial information, and medical information. This information is accorded protection, usually by law, because it is considered highly personal no matter what the context or situation. Other information may be protected because the *context*, or *circumstances*, of its collection, use, maintenance, or release has violated an accepted custom, such as:

- When the proposed use, maintenance, or collection of the information violates parameters the individual set when giving access to the information. For example, an employee may release information justifying the use of personal leave time, but a privacy interest is raised if the employer shares with others that the employee spent the day at a weight-loss program or the racetrack.
- When the collection of information is surreptitious, such as hidden cameras in a public place. In this situation, the person is releasing personal behavior information without the ability to establish the condition for its use because of the lack of knowledge that it is being collected. Biometric data, which can be collected without any physical contact, may particularly raise this concern.
- When the maintenance of the information differs from what is ordinarily expected or from its implicit purpose. For example, people are accustomed to passenger manifests and customs searches, but the sharing of this information for the purposes of collecting data on travel companionship and what books people have in their baggage could implicate a privacy interest because of the unexpected use of the information and the implicit limitation that customs searches are only for the purpose of discovering prohibited objects.
- When the release of the information differs from the implied use. For example, the United States Supreme Court had to decide, in *Doe v. Reed*, whether signatures collected on a petition in Washington State could be publicly released; even though the petition signers knew the signatures would be scrutinized by public officials, they asserted a privacy interest in blocking the information from being available to the public at large.

4.1.3 How Do Privacy Issues Arise?

Privacy *concerns* are generated when PII is collected, used, maintained, or released in a way that is inconsistent with the expectation of the person to whom the information belongs. A privacy *interest* is affected when that expectation is grounded in law or custom, not simply the person’s desire to prevent the offending intrusion. For example, many people might prefer that their residential address not be available on a public tax assessor’s Web site if they own a home; however, there is no law precluding publication, and that information has historically been deemed public. In this example, the person has a privacy *concern* about the collection, use, maintenance, and release to the public of the information but no cognizable privacy *interest* other than the quality of the information (refer to Section 4.3). It is

important to reiterate, accommodation of privacy *concerns* that do not rise to cognizable *interests* or *rights* is outside the scope of this policy.

In today's information sharing environment, well-developed privacy, civil rights, civil liberties, and IQ policies help an agency prevent problems. Failure to develop, implement, and maintain such dynamic policies can result in:

- Harm to individuals.
- Public criticism and loss of confidence in and cooperation with the agency.
- Lawsuits and liability.
- Limited ability to share information.
- Proliferation of agency databases with inaccurate data.
- Damage to the credibility of agencies that act on inaccurate data.

The PII maintained by entities—if handled inappropriately—can cause problems for those affected. In worst cases, personal safety may be jeopardized. These issues affect the whole justice community, including law enforcement, prosecution, defense, courts, parole, probation, corrections, and victim services, as well as members of the public having contact with the justice system.

Unless effective privacy, civil rights, civil liberties, and IQ safeguards are being utilized at every level of your agency's information and data-handling operation, you may be exposing yourself and others to unacceptable risks from inaccurate information or problems caused by failure to honor essential protection expectations. When agencies collectively maintain appropriate levels of attention to privacy, civil rights, civil liberties, and IQ, the sharing of information is facilitated in a responsible and effective manner.

4.1.4 Factors Influencing Whether Information Sharing Implicates Privacy Interests

The existence and strength of privacy interests is not binary. In other words, it cannot be represented directly by answering yes or no to equally strong interests. In addition, the extent to which a privacy interest is honored will depend both on its strength and the type and weight of the interest of the agency in the collection, use, maintenance, and release of the information. A number of factors influence both the existence and strength of a privacy interest, such as:

- Whether the information is ordinarily exposed to public view. The line between public and limited exposure has become particularly blurry with the advent of social networks and other sites dedicated to the exchange of information. People may assume that distribution is limited to a narrower group than in fact has access to the information.⁹
- Whether the collector of the information is a public or private entity. This is relevant on at least two levels. First, information collected by a public agency is often thought of as presumptively open to the public, and some statutes and regulations codify this expectation. Second, it may generally be assumed that collection of data by public entities is more intrusive than collection by private concerns.¹⁰
- Whether the collection of the information is patent or surreptitious.
- Whether the information was collected from targeted individuals in response to a specific incident or, at the other end of the spectrum, collected from a large group randomly or en masse.
- The extent to which the surrender of the information is free or is influenced by the exercise of a right or privilege and, if so, the importance of the right or privilege. Essentially, this consideration focuses on the broad area between “optional” and “required.” For example, much information is surrendered in order to obtain a driver's license or to travel. Because of the importance of driving and traveling

⁹ For example, see “Privacy, Free Speech and ‘Blurry-Edged’ Social Networks,” *Boston College Law Review*, Vol. 50, No. 5, 2009.

¹⁰ An inquiry outside the scope of this discussion is whether individuals serving public roles have fewer or different privacy interests than those operating in the private sector. For example, some states publicize the salaries of public officials, which is information that in the private sector is generally not disclosed.

in American society, the use of that information may be more strictly governed than the use of data surrendered in order to attend a rock concert.

- The extent to which the expectation of the individual is grounded in law versus custom and, if in custom, the universality of the custom.
- How limited the use of the information will be and how tailored the use is to the purpose of collection.
- Whether the information will be stored at all and, if so, for how long a period.
- How available the data will be, on a scale between authorized users in a controlled setting all the way to public access.
- The extent of laws regulating the use, maintenance, and retention of the data once collected and the security of the maintenance of the data.
- The extent to which the data includes information about “bystanders,” as with a group photograph, or about “witnesses” or “nonsuspects” as with the use of “familial DNA,” for example.

These are but some of the factors influencing whether a privacy interest is implicated and, if so, whether the collection, use, maintenance, and release of the information should be governed by a privacy policy. As technology has expanded our concerns about privacy and our fears of inappropriate use of data, so will continuing developments influence our decision making about how privacy should be protected.

4.2 What Are Civil Rights and Civil Liberties?

The term “civil liberties”¹¹ generally means the freedom from intrusive or undue government interference, while “civil rights”¹² refers to the rights of individuals to participate fairly and equally in society and the political process. Civil liberties are generally spoken of in the negative—what government cannot do—whereas civil rights are generally positive¹³ (or affirmative)—what the government must or should do to ensure equality and fairness. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference. Privacy is coupled more naturally with civil liberties because privacy is a concept about prohibiting certain intrusions.

4.2.1 How Do Civil Rights and Civil Liberties Issues Arise?

Civil liberties issues most commonly arise when the government intrudes or proposes to intrude into individual affairs in a way that is counter to law, regulation, or accepted practice; when it exceeds its lawful authority in attempting to control individual behavior; or when the criteria for the collection or sharing of information are based solely on constitutionally protected activities or categories.

In the information sharing context, numerous potential civil liberties issues arise when government collects, uses, maintains, and disseminates personal data; for example, if the government collects irrelevant information that is broader than necessary to address the specific purpose for which it is being sought or collects it for one purpose and then uses it for another. Civil liberties issues are also implicated when the government disseminates collected information to other government entities or private parties without the individual’s knowledge or consent. Civil liberties issues may also arise in the context of what information about an individual the government should be able to obtain from private sources and the legal standard under which that information can be obtained (e.g., under what conditions and standards may the government obtain cell phone or Internet subscriber records). In addition, civil liberties issues arise when the government fails to provide a meaningful avenue for the individual whose information

¹¹ 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.

¹² 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.

¹³ “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.

has been collected to be able to examine his/her own file to determine whether there are any errors and be able to correct them or to learn whether third parties have been provided access to the information. A pressing civil liberties issue in the post-9/11 environment is the increased aggregation of numerous pieces of information about individuals, from sources both public and private. Although the individual pieces of information may not, by themselves, amount to an intrusion of privacy, their aggregation into a centralized “cradle to grave” dossier creates significant civil liberties concerns.

Civil rights and civil liberties are also implicated when sharing information that was collected regarding activities that are protected by an individual’s free exercise. Government may not collect or retain information based solely on First Amendment-protected activities or conduct investigations on that basis. Even when information regarding First Amendment-protected activities is collected, government must be careful to limit its collection to that information which is both necessary and legally authorized.

4.3 What Is Information Quality (IQ)?

Traditionally, “information quality” is defined as the accuracy and validity of the actual content of the data, data structure, and database/data repository design. Conventional wisdom typically equates good information with accurate information. Good information, however, should also be timely, reliable, and complete. Today, IQ is understood to be a multidimensional concept that encompasses critical relationships among multiple attributes, such as timeliness, accuracy, relevancy, and others. Together, these attributes contribute to the validity of the information. Quality information is the cornerstone of sound entity decision making and inspires trust in the justice system and in the law enforcement entities that use information. Such information enables entities to perform their jobs efficiently and effectively.

4.3.1 How Do Information Quality Issues Arise?

Poor information quality can be harmful to the individual, the community, and the justice entity.

Failure to actively and continuously evaluate and improve IQ in justice-related information sharing practices may result in harm or injustice to individuals, lawsuits and liability, population of other entity databases with inaccurate data, public criticism, inefficient use of resources, or inconsistent actions within entities. As discussed in Section 4.3.2, poor IQ intersects privacy, civil rights, and civil liberties concerns.

The routine nature of day-to-day business processes underscores the potential for inadvertent generation of inferior IQ. As information is increasingly shared and becomes more readily and rapidly accessible electronically, justice entity control over IQ becomes a bigger challenge. The typical triggers for poor IQ are commonplace business challenges, such as:

- Bypassing data input rules and too restrictive data input rules.
- Changing data needs from information consumers.
- Coded data from different functional areas.
- Complex data representations, such as text and image.
- Data cleansing, normalization, standardization, and processing.
- Delays.
- Distributed heterogeneous systems.
- Failure to update record information.
- False information provided (more than name).
- Human error (e.g., transposition, translation, carelessness).
- Improper releases of information.
- Incomplete records.

- Large volumes of data.
- Limited computing resources.
- Multiple entries (e.g., where aliases are used).
- Poor integration of data from multiple data sources and erroneous linking of information.
- Security-accessibility trade-off.
- Subjective judgment and techniques in data production/collection.
- Technical issues.
- Widespread availability of data (part of day-to-day business issues encountered by justice entities).

4.3.2 Privacy and Information Quality

This guide addresses the development of privacy policies to ensure proper gathering and sharing of accurate PII. Justice entities must recognize that despite the implementation of an effective policy, damage and harm can still occur if the underlying information is deficient in quality.

Information quality plays an extremely important role in the protection of privacy rights of individuals. Issues of privacy and IQ are inherently linked since both concepts share multiple information attributes that influence appropriate treatment of PII. Entity privacy policies should address IQ issues. Information quality is specifically enumerated as an issue to be considered in the Fair Information Principles—Data Quality Principle: Personal data should be relevant to the purposes for which it is to be used and, to the extent necessary for those purposes, should be accurate, complete, and up to date (refer to Section 8.3.1.2, Information Quality Relative to Collection and Maintenance of Information). In practice, the accuracy, completeness, currency, and reliability of information connected to an individual may raise as many concerns as the release of the information or its public availability.

4.4 What Is Security?

PII needs to be protected with reasonable safeguards against risk of loss or unauthorized access, modification, use, destruction, or disclosure. Information systems should provide the controls to prevent, detect, and respond to threats and vulnerabilities that may compromise the integrity of the information systems.

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.

4.4.1 How Do Security Issues Arise?

Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording, or destruction is an important part of security. Security issues can arise when entities have:

- Unsecure facilities and networks that are vulnerable to external intrusion.
- Unsecure internal and external safeguards.
- Unsecure information storage formats, making it easier to modify, access, or destroy information.
- Undefined access permissions, meaning all users have access to all information, resulting in loss of control over what information a particular group or class of users can have access to or their established permissions (e.g., who can view, add, change, delete, or print).

- Poor (or nonexistent) audit logs where essential access, or query, information—such as the identity of the user and what information was searched, accessed, modified, or disseminated—is not tracked.
- Risks of data breach—the unintentional release of secure information to an untrusted environment.

4.4.2 Privacy and Security

Although privacy and security both relate to the handling of data and information and are both essential to justice-related information sharing, they have different implications and considerations. Security relates to how an organization protects information during and after collection. Privacy addresses why and how information is collected, handled, and disclosed and is concerned with providing reasonable quality control regarding that information. Security policies implement privacy policies by ensuring compliance with the manner and extent to which information is allowed to be shared by the privacy policies. Having a security policy related to data or information is not enough. Security policies alone do not adequately address the privacy, civil rights, civil liberties, and IQ issues contemplated in this discussion. Considering the breadth of the issue, some existing privacy policies may fail to address these concerns in that they relate to access to records instead of defining privacy protections both in procedures and in system processes.

A privacy policy is different from a security policy. A security policy carries out the privacy policy and therefore may be incorporated within a privacy policy, but by itself, it may not adequately address the protection of PII or the requirements of a privacy policy in its entirety. The Global Security Working Group (GSWG) has developed a product titled *Applying Security Practices to Justice Information Sharing*¹⁴ to address security practices.

An effective privacy policy should describe how security is implemented within the integrated justice system for the purposes of protecting PII. Similarly, a security policy should address information classification, protection, and periodic review to ensure that information is being stewarded in accordance with an organization's privacy policy.

4.5 Relationship Among Privacy, Information Quality, and Security

While privacy is related to and overlaps with IQ and security, each also has distinctly different issues that must be addressed and that may require distinct solutions. As such, these topics merit separate attention and are addressed in related Global products. See Section 4.8 for a list of these products.

4.6 What Is a Privacy Policy?

A privacy policy is a written, published statement that articulates the policy position of an organization on how it handles the PII and other personal, sensitive information it seeks or receives and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, dissemination, access, expungement, and disposition.

Privacy policies relate to the role of government and how government entities conduct themselves. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference in the conduct of their lives. The purpose of a privacy policy is to articulate (within the organization, to external entities that access and share information with the organization, to other entities, and publicly) that the entity will adhere to legal requirements and entity policy and procedural provisions addressing the gathering and sharing of information in a manner that protects constitutional and statutory rights, including personal privacy and other civil liberties and civil rights. A well-developed and implemented privacy policy uses justice entity resources prudently and effectively; protects the entity, the individual, and the public; and contributes to public trust and confidence that the justice system understands its role and promotes the rule of law.

¹⁴ Global Security Working Group (GSWG), Global Justice Information Sharing Initiative (Global), *Applying Security Practices to Justice Information Sharing*, Version 4.0, May 2007, <http://it.ojp.gov/documents/asp/>.

4.6.1 When Should an Entity Develop a Privacy Policy?

A privacy policy is an essential ingredient of sound information management. Therefore, the optimal time to develop a policy is in the planning and development stages of a justice information sharing system. Although not optimal, a privacy policy may also be developed during or after implementation of any information-gathering practice. The important goal is to have a policy in place.

4.7 Preparation for a Privacy Policy—the Privacy Impact Assessment (PIA)

A Privacy Impact Assessment (PIA) is a vital tool used to evaluate possible privacy risks and to mitigate identified risks to the privacy, civil rights, and civil liberties of individuals while maximizing technological infrastructures and data sharing opportunities. A PIA allows justice practitioners to examine the privacy implications of their information systems and information sharing collaborations so they can design and implement policies and procedures to address vulnerabilities and protect PII and other personal, sensitive information to ensure that it is not improperly collected or distributed.

4.7.1 When to Perform a PIA?

Privacy concerns must be addressed as part of an overall strategic planning process for information systems' development, enhancement, and replacement or any time a system is modified, updated, and/or revised. Committees formed to oversee planning and implementation should, ideally, make conducting a PIA their first step, followed by the development of privacy policies that are based on information obtained during the assessment process. However, a PIA can be conducted at any time or when the information sharing process is being changed or expanded.

Privacy policies emerge through the identification and analysis of the PIA process, generating discussion and decision making on how to address and mitigate, if necessary, the identified privacy vulnerabilities. The PIA is a road map for developing a thoughtful and comprehensive privacy policy to protect personal and confidential information, to serve the needs of the entity and the public.

4.7.2 PIA Template

The Global ***Guide to Conducting Privacy Impact Assessments for State, Local, and Tribal Justice Entities*** (www.it.ojp.gov/privacy) contains a PIA template that leads policy developers through appropriate privacy risk assessment questions that evaluate the process through which PII is collected, stored, protected, shared, and managed by an electronic information system or online collection application.

4.8 Resources

4.8.1 Privacy Resources

- **Global Privacy Resources booklet:** The following GPIQWG privacy resources, including this Privacy Guide, are featured in the booklet and available online at www.it.ojp.gov/privacy.
 - *Executive Summary for Justice Decision Makers: Privacy, Civil Rights, and Civil Liberties Program Development*, Appendix A.1 of this guide.
 - *7 Steps to a Privacy, Civil Rights, and Civil Liberties Policy*, Appendix A.2 of this guide.
 - *Guide to Conducting Privacy Impact Assessments for State, Local, and Tribal Justice Entities*.
 - *Privacy, Civil Rights, and Civil Liberties Policy Development Template for State, Local, and Tribal Justice Entities*, Appendix C.1 of this guide.
 - *Privacy, Civil Rights, and Civil Liberties Policy Development Guide for State, Local, and Tribal Justice Entities: Policy Review Checklist*, Appendix D of this guide.
- Smith, Robert Ellis, *Ben Franklin's Web Site: Privacy and Curiosity From Plymouth Rock to the Internet*, 2000, ISBN 0-930072.

- U.S. Department of Justice’s and U.S. Department of Homeland Security’s Privacy and Civil Liberties Portal—Issues, Resources, and Training for Fusion Centers and State, Local, and Tribal Justice and Public Safety Agencies, www.it.ojp.gov/PrivacyLiberty.
- U.S. Department of Homeland Security, Office for Civil Rights and Civil Liberties, www.dhs.gov/about/structure/crcl.shtm.
- U.S. Department of Homeland Security, Privacy Office, www.dhs.gov/xabout/structure/editorial_0338.shtm.
- U.S. Department of Justice, Privacy and Civil Liberties Office, www.usdoj.gov/pclo/.
- Office of the Program Manager, Information Sharing Environment (ISE), *Privacy, Civil Rights, and Civil Liberties Protection Framework*, www.ise.gov/privacy-civil-rights-and-civil-liberties-protection-framework.

4.8.2 Information Quality Resources

Global Information Quality Series: The following resources offer practical guidance on how to make IQ a priority and how to establish and implement an entity-wide IQ program. All of these resources are available for download at: www.it.ojp.gov/IQ_Resources.

- ***Information Quality: The Foundation for Justice Decision Making***

Good IQ is the cornerstone for sound entity decision making and inspires trust in the justice system and in the law enforcement entities that use information. With that view in mind, DOJ’s GPIQWG released a primer on IQ, entitled *Information Quality: The Foundation for Justice Decision Making*.

This resource is targeted towards justice leaders and justice information sharing system administrators and emphasizes the importance of good, or “quality,” data that enables entities to perform their jobs efficiently and effectively. The justice system depends on information sharing. With the rapid proliferation and evolution of new technologies, increased data sharing requires increased responsibility for IQ to ensure sound justice decision making. This fact sheet explores information quality as a multidimensional concept encompassing critical relationships among multiple attributes, such as timeliness, accuracy, and relevancy. Hypothetical scenarios are presented depicting situations of good and poor IQ, as well as suggestions on what entities can do about IQ. Research and resource references are also provided for further reading.

- ***9 Elements of an Information Quality Program***

Developed for high-level, managerial, and administrative personnel within an organization, *9 Elements of an Information Quality Program* introduces the nine key steps of an entity-wide IQ program.

- ***Information Quality Self-Assessment Tool***

A mandatory step for any entity in developing an IQ program is the completion of an IQ self-assessment—the evaluation of entity information and reports associated with justice events. The *Information Quality Self-Assessment Tool* will help entities determine their relative level of IQ and benchmarks for evaluation, improvement, and accountability. Using this tool can:

- Break down the flow of information in a justice event into the multiple phases of an information life cycle.
- Apply IQ dimensions to each point along this information continuum.
- Uncover gaps in roles, responsibilities, policies, procedures, and technology that beget IQ problems.
- Implement IQ in practice.
- Enhance overall understanding of the effects that a justice entity’s business processes—related to information collection, maintenance, management, dissemination, and disposition—have on IQ.

- **Information Quality Program Guide**

The *Information Quality Program Guide* is intended to help managers of justice information systems develop an IQ program for their organizations and is designed to support those who must analyze their justice entity's information and determine what is needed to ensure good quality information. The guide features a step approach to the development and implementation of an entity-wide IQ program by leading practitioners through the:

- Establishment of IQ as an entity-wide program.
- Identification and analysis of entity justice events and products.
- Application of standard and customized IQ dimensions.
- Completion of an IQ assessment.
- Implementation and follow-up.

The following is a list of IQ resources currently in publication. Additional resources are also available at www.it.ojp.gov/IQ_Resources.

- Bureau of Justice Statistics, *Data Quality Guidelines*, <http://bjs.ojp.usdoj.gov/content/dataquality/dataquality.cfm>
- Bureau of Justice Statistics, *Quality Guidelines Generally Followed for Police-Public Contact Surveys, but Opportunities Exist to Help Assure Entity Independence*, http://it.ojp.gov/documents/BJIS_DQ_Guidelines_Police_Public.pdf.
- English, Larry P., *Improving Data Warehouse and Business Information Quality*, John Wiley and Sons, New York, 1999, www.infoimpact.com/book.cfm.
- English, Larry P., "The Essentials of Information Quality Management," *DM Review*, September 2002.
- Federal Bureau of Investigation's Criminal Justice Information Services, *Methods of Data Quality Control: For Uniform Crime Reporting (UCR) Programs*, http://it.ojp.gov/documents/CJIS_Methods_of_DQ_Control_for_UCR.pdf.
- Fisher, Lauria, Chengalur-Smith, and Wang, Massachusetts Institute of Technology, Information Quality Publication, *Introduction to Information Quality*, <http://mitiq.mit.edu/Books.htm>.
- INFORMATICA White Paper, *Monitoring Data Quality Performance Using Data Quality Metrics*, http://it.ojp.gov/documents/Informatica_Whitepaper_Monitoring_DQ_Using_Metrics.pdf.
- Massachusetts Institute of Technology (MIT), Total Data Quality Management (TDQM) Program and International Information Quality (IQ) Conference, <http://web.mit.edu/tdqm/www/index.shtml>.
- Office of Management and Budget's (OMB) Office of Information and Regulatory Affairs, Web Resource for Information Quality Guidelines, www.whitehouse.gov/omb/inforeg_agency_info_quality_links.
- U.S. Department of Justice, Information Quality Guidelines, www.usdoj.gov/oig/FOIA/guidelines.htm.
- U.S. Department of Justice's Office of Community Oriented Policing Services (COPS), Information Quality Guidelines, www.cops.usdoj.gov/Default.asp?Item=1654.
- Wang, Richard Y., Yang W. Lee, Leo L. Pipino, and Diane M. Strong, "Manage Your Information as a Product," *Sloan Management Review*, Massachusetts Institute of Technology, Summer 1998, Volume 39, Number 4.

4.8.3 Security Resources

- Global Justice Information Sharing Initiative (Global) Security Working Group (GSWG), *Applying Security Practices to Justice Information Sharing*, Version 4.0, May 2007, <http://it.ojp.gov/documents/asp/>.

- GSWG, Implementing Privacy Policy in Justice Information Sharing: A Technical Framework, October 31, 2007, [www.it.ojp.gov/documents/Privacy_Report_ReleaseCandidate_v_1_0_10-31-2007_with_cover_\(final\).doc](http://www.it.ojp.gov/documents/Privacy_Report_ReleaseCandidate_v_1_0_10-31-2007_with_cover_(final).doc).
- IJIS Institute, *Information Security in Integrated Justice Applications: An Introductory Guide for the Practitioner*, www.it.ojp.gov/documents/info_fsec_guide.pdf.
- Safeguarding Against and Responding to the Breach of Personally Identifiable Information, Office of Management and Budget Memorandum M-07-16 (May 2007), www.whitehouse.gov/OMB/memoranda/fy2007/m07-16.pdf.
- SEARCH, The National Consortium for Justice Information and Statistics, prepared for the Office of Community Oriented Policing Services, U.S. Department of Justice, *Law Enforcement Tech Guide for Information Technology Security: How to Assess Risk and Establish Effective Policies—A Guide for Executives, Managers, and Technologists*, www.search.org/files/pdf/ITSecTechGuide.pdf.
- SEARCH, The National Consortium for Justice Information and Statistics, SEARCH IT Security Self- and Risk-Assessment Tool, www.search.org/files/xls/SEARCHITSecurityAssessmentTool.xls.

Section 5—Assembling the Project Team

A privacy policy requires individuals to oversee its development, implementation, and currency. This section describes the roles and responsibilities of those persons who create, produce, implement, and oversee the policy described in this publication. It is important to have the structure and support for the planning effort clearly defined from the outset.

5.1 Identifying the Project Champion or Sponsor

Once the need for a privacy policy is established, the next step is to designate a high-level project champion or sponsor within the organization to drive the effort. The project champion will be the individual who will help steer the development of the policy, identify and allocate the necessary resources (both human and other support), and oversee policy implementation. The project champion or sponsor should:

- Advocate for and defend the effort, the project team leader (refer to Section 5.3), and the team.
- Empower the team and its leaders with appropriate authority.
- Ensure that adequate and appropriate resources are available to the team.
- Remove obstacles and address political and organizational issues.
- Support the team on policy issues.
- Act as the high-level authority for the effort.
- Articulate and share the common goals of the effort.

The project champion or sponsor can be:

- The person who designates the project team leader, someone higher in the chain of command who is in a position to facilitate decision making and resource allocation.
- The highest-ranking officer in the particular justice entity.
- The Governor of a state or a tribal leader.



In the case of a collaborative effort in which the ultimate policy may be adopted by more than one organization, there may be champions from each organization who will be bound by the completed policy statements.

Selection of the project champion or sponsor for this development effort will depend entirely on factors specifically related to the assignment and the organization. The key to identifying the project champion is not only to recognize the need for a sponsor but to identify what role the champion will serve. This person should provide a strong voice for the team effort, particularly when there is competition for scarce resources. The champion should also provide the mechanism for efficient decision making when the project team leader or project manager does not have the authority to make decisions in selected areas.

5.2 Securing Support and Justifying Resources

5.2.1 Securing Agency Head Support

Securing approval and buy-in for a privacy program, project team, and the policy and implementation efforts that will result requires top-down support. One way to obtain this support is to raise awareness among agency heads of the importance of privacy protections and the risks and liability of not having the right protections in place in agency policies and day-to-day procedures. This guide contains two executive-level summaries, described below, in Appendix A. These can help an agency make the case for a privacy protections policy.

5.2.1.1 *Executive Summary for Justice Decision Makers: Privacy, Civil Rights, and Civil Liberties Program Development*

This executive summary is an awareness resource for justice executives, as well as an informational tool to use for training. The easy-to-read flyer is designed to engender awareness about the topic, make the case for privacy policy development, and underscore the importance of promoting privacy protections within justice agencies. Included is information on basic privacy concepts; the intersection between privacy, security, and information quality; privacy risks; and steps to establish privacy protections through a privacy program cycle. This paper applies settled privacy principles to justice information sharing systems and makes recommendations on best practices.

5.2.1.2 *7 Steps to a Privacy, Civil Rights, and Civil Liberties Policy*

Designed for both justice executives and agency personnel, this document raises awareness and educates readers on the seven basic steps involved in the preparation for development of a privacy, civil rights, and civil liberties policy (as recommended in this Privacy Guide). Each step describes the practical tasks associated with preparing for, drafting, and implementing a privacy policy. Also featured is an overview of the core concepts (or chapters) that an agency should address in the written provisions of a privacy policy (as recommended in the SLT Policy Development Template).

5.2.1.3 *The Importance of Privacy, Civil Rights, and Civil Liberties Protections in American Law Enforcement and Public Safety. Line Officer Training Video*

A training video titled *The Importance of Privacy, Civil Rights, and Civil Liberties Protections in American Law Enforcement and Public Safety* was developed by Global's Intelligence Working Group (GIWG) Privacy and Training Committees. This short video is a training tool designed to educate viewers, particularly line officers during roll call, on the privacy and civil liberties issues they may confront in their everyday work and the liabilities associated with the failure to adhere to sound policy and practice. This video can be viewed online at www.ncirc.gov/privacylineofficer, or to request a copy, contact Global@iir.com.

5.2.2 Justifying Resources

Any policy development team must make an estimation of resource needs and make those resource needs known to the project champion. Different resources may be needed at different phases of the effort. At a minimum, however, the team should project a realistic estimate of resource needs, including:

- Number and needed skill sets of team members required to successfully work on the project.
- An approximate number of hours necessary to complete the project.
- A list of any additional support resources that may be necessary (for example, computers, software, and access to legal services).

While this estimate may change, it will be beneficial to provide the project champion and organization with basic information about resource needs in order to assist the organizational assessment of resource allocation. Providing this estimate should result in an articulated response from the organization's management about what resources will or will not be made available for this project.

In determining resource needs, the following questions may be helpful in preparing for a resource justification:

- How many team members will be needed or available from the initiating organization and other organizations?
- What types of resources are needed to support a privacy policy development team (for example, skills or interests of team members, meeting facilities, hardware and software, other equipment, and technical support and legal support)?
- Can resources be reallocated within the entity?
- What other support (staff, travel, materials, or contract support) will be needed?
- What training, if any, is available or needed?
- Are the identified resources available within the initiating organization or from other organizations, and who has authority over these resources?
- If not, what are other potential sources of the needed resources, and what approaches can be used to obtain them? Who has authority over these resources, and will the project champion support these requests?

In the initial stages of development, not all of these questions may be answerable, but going through the process of addressing such questions will help to define what is or is not available and may be useful, as the project progresses, in supporting future requests for needed resources.

5.3 Identifying the Project Team Leader

The privacy policy development project must have a project team leader—someone who will direct and manage the project on a day-to-day basis. Generally, the individual assigned to read this guide may have been designated as the project team leader. In any event, the project team leader should possess the following essential characteristics:

- **Organizational Credibility**

The project team leader should be in a position of credibility within the organization and with outside entities essential to the success of developing and implementing privacy policies. This does not necessarily mean that this individual possesses an in-depth knowledge of every technology-, privacy-, and civil liberties-related issue. This individual should, however, understand the technological applications for justice information sharing and the limitations of these applications, as well as the organization's work flow, specifically as it involves the control of data.

- **Organization Authority**

The project team leader should be in a position to access resources (human and financial) necessary to complete the task and to obtain needed approval or direction from the project champion and the organization's chief executives.

- **Ability to Build and Manage Coalitions**

Since success in this endeavor depends on the substantive involvement of a number of individuals within the department and from outside entities, the project team leader's ability to build and manage coalitions is essential. The foundation of this ability is the art of managing human relationships—making sure that individual needs are met in the process of accomplishing the ultimate goal of developing and implementing privacy policies that affect multiple justice entities.

- **Ability to Manage Day-to-Day Tasks Over an Extended Period of Time**

The process of developing privacy policies will take a significant amount of effort over an extended period of time. It is essential for the project team leader to be able to manage the day-to-day policy development activities, under what is probably minimal human and financial resources, as well as set and adhere to timelines and maintain focus on the ultimate goal.

5.4 Building the Project Team and Stakeholder Contacts

Presumptively, a collaborative project team should be appointed to develop the privacy policy. Collaborative teams function best when participant roles and responsibilities are clear.

5.4.1 Project Team

Appointing a multidisciplinary, multientity team is necessary to develop and implement successful privacy policies. This type of collaboration lends a wide range of viewpoints, substantive knowledge, and energy to a process that can easily be bogged down in details and differing interpretations and objectives. To succeed, this team needs structure, leadership, and a sense that the goal can be accomplished.

It is important to establish a clear decision-making process that recognizes and values individual participation. This process should allow for diverse input yet move towards achieving the stated policy goal. While the project team should represent a broad array of perspectives, it is important that the number of team members be kept to a manageable size to ensure that the team can accomplish its goals and objectives. Team members must represent the core entities that are entrusted with the protection of private information for justice information sharing.

The project team should have access to subject-matter experts in areas of privacy law and technical systems design and operations, as well as skilled writers, but these individuals do not necessarily have to be team members.

5.4.2 Stakeholder Contacts

Stakeholder contacts are entities or individuals essential to the development and implementation of the policy but who may or may not be on the project team. Stakeholders have interests in the outcome of the privacy policy and are solicited by the project team to provide input.

Carefully consider what entities and individuals are essential to developing and implementing the policy.

Determine some method for obtaining input from stakeholders. Methods for obtaining stakeholder input can include focus groups, surveys, documents for public comment, and invitations to speak on varied issues at team meetings.

In determining the composition of the project team, it may be helpful to divide potential stakeholders into those who may implement the policy, those who are affected by the policy, or those who have a vested interest in the policy:

- Entities participating in information sharing, local or state lawmakers or tribal leaders, and the legal community (judges, prosecutors, and defense attorneys).
- Community members, offenders and their families, victims of crime, and employees of entities involved in justice information sharing, as well as nonjustice entities who require access to justice information. Carefully consider the local justice information sharing environment and determine whether it is advantageous to include representatives from some of these groups on the project team.
- The public at large, academia, commercial data consolidators, and private security organizations. At a minimum, information should be made available concerning privacy policies to these groups. In addition, victim rights advocates, privacy advocates, and the media can also affect the development and implementation of policies for justice information sharing.

5.5 Continuing Roles Within the Entity

5.5.1 Privacy Officer

Though the project champion and project team will direct the development of the privacy policy and implementation plan, the task of continued implementation, monitoring, and compliance should be guided by a Privacy Officer. During the project team selection process, one individual should be selected to serve as the entity's Privacy Officer during policy development and as an ongoing role. This individual may or may not be the same person designated as the project champion or project team leader. Ultimately, once the policy has been completed, the Privacy Officer will maintain primary oversight and managerial responsibility for ensuring continued policy implementation, training, monitoring, and compliance. Traditional Privacy Officer responsibilities include:

- Routinely review the entity's information privacy procedures to ensure that they are comprehensive and up to date.
- When additional or revised procedures may be called for, work with relevant entity offices in the consideration, adoption, and implementation of such procedures.
- Review existing departmental and component-level privacy policies and procedures to ensure the entity's full compliance with local, state, and federal laws, regulations, and policies relating to information privacy.
- Oversee the implementation of privacy protections in personnel procedures and information system processes.
- If applicable to the entity's function, review and approve all analytical products for appropriate privacy, civil rights, and civil liberties protections prior to dissemination or sharing by the entity.
- Handle reported errors and violations of the provisions of the privacy policy.
- Ensure that enforcement procedures and sanctions (which should be outlined in the privacy policy) are adequate and enforced.
- Receive and respond to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s) maintained or accessed by the entity.
- Manage the evaluation of user compliance (for example, through the use of system audits).
- Serve as a point of contact for handling individuals' requests for corrections involving information the entity has disclosed and can change because it originated the information. The Privacy Officer will inform individuals of the procedure for requesting and considering requested corrections, including appeal rights.

5.5.2 Security Officer

Justice information sharing entities must ensure that appropriate security measures are in place for the data that is collected, stored, accessed, and maintained by the entity, as well as for the facility and entity personnel. Oversight of this assurance should be assigned to a security officer. As referenced in Section 4.4.2, Privacy and Security, privacy risks can occur as a result of inadequate security measures.

Privacy and security are inherently linked. For example, if access to information contained in the justice information system is not restricted, the privacy rights of individuals may be affected. Further, if the system network is not secure and well protected from external intrusion, individual harm may result. Assigning the role of a security officer within the entity will help support privacy protections through clear responsibility for the coordination, development, implementation, and maintenance of security policies and procedures. A security officer will ensure that:

- The agency operates in a secure facility protected from external intrusion.
- Information is stored in a secure format and secure environment such that it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions.
- Access to information is granted only to personnel whose positions and job duties require such access (e.g., who have successfully completed a background check and appropriate security clearance, if applicable, and who have been selected, approved, and trained accordingly).
- Queries made to the agency's data applications are logged into the data system identifying the user initiating the query.
- System logs are kept of accessed and disseminated agency data and an audit trail is maintained.
- Procedures are established and followed for breach notification laws or policies.

A security officer may also:

- Conduct security training and awareness of the agency's security policies, including security measures, policies, and procedures.
- Provide regular updates to the agency's management and governance body on compliance with security policies.
- Coordinate with federal security officials, if applicable, to the extent needed to facilitate federal security clearances for personnel, facility security, certifications, and access to federal information systems.
- Establish and coordinate the processes used to conduct background checks on all agency personnel prior to commencement of duties.
- Receive, document, and investigate reports of security violations according to the agency's security policies.

5.6 Resources

- Beyerlein, Michael M., and Cheryl Harris, *Guiding the Journey to Collaborative Work Systems: A Strategic Design Workbook*, San Francisco: Pfeiffer Press, 2003.

This is a hands-on, practical guide for dealing with the challenges of designing and implementing collaboration in the workplace. The workbook covers a broad range of topics necessary for successful change, including generating and maintaining support for the initiative, launching a thoroughly planned change program, and effectively communicating the plan to the rest of the organization. Filled with assessments, tools, and activities and based on interviews conducted with 21 experts and hundreds of team members, *Guiding the Journey to Collaborative Work Systems* offers the support needed to design in-depth plans for changing work systems to facilitate collaborative excellence.

- Clark, Donald, *Teamwork Survey*, 2004, www.nwlink.com/~donclark/leader/teamsuv.html.

This is a questionnaire used to evaluate the effectiveness of how a team operates.

- Cook, Ian, The Center for Association Leadership, White Paper: *Kickstarting a Brand New Team*, January 2002, www.asaecenter.org/PublicationsResources/whitepaperdetail.cfm?ItemNumber=12185.

This is an article on what to do and what to avoid when creating, managing, and leading a new project team.

- Francis, David, and Don Young, *Improving Work Groups: A Practical Manual for Team Building*, Revised Edition, San Francisco: Jossey-Bass/Pfeiffer Publishers, 1992.
- Graham, Robert J., and Randall L. Englund, *Creating an Environment for Successful Projects*, 2nd Edition, San Francisco: Jossey-Bass Publishers, 2003.
- *Improving Work Groups: A Practical Manual for Team Building* contains guidelines and 25 activities designed to build and maintain effective teams. Aimed at any manager, consultant, or employee responsible for developing effective teams, this publication offers a step-by-step system for initiating and evaluating team performance.
- National Criminal Justice Association (NCJA), Survey of State Governance Structure, *States' Governance of Justice Information Systems Integration: Managing Decisionmaking in an Integrated Environment*, June 2001, www.nga.org/cda/files/STATESGOVJUSTICE.pdf.
- Team Building Associates, *The Strategic Approach: Six Stages to Higher Performance*, <http://teambuilder.server101.com/strategicteambuilding.htm>.

This report is a brief review of the required elements for an effective team.

- The following documents can be obtained from American Indian Development Associates, 2401 12th Street, NW, Suite 212, Albuquerque, New Mexico 87120, (505) 842-1122, e-mail Info@aidainc.net:

2004 Charter for the New Mexico Crime Data Project.

Melton, A. P., and S. Wall. Integrated Justice Systems in American Indian Communities Planning Series: *Intergovernmental Agreements Supporting Crime Information and Exchange Among Tribes and States*, 2004, www.aidainc.net/Publications/index.htm.

Melton, A. P., S. Wall, and H. Lewis. Integrated Justice Systems in American Indian Communities Planning Series: *Understanding the Tribal Justice and Law Enforcement Environment*, 2004, www.aidainc.net/CRD%20Envir.pdf.

- The following resources can be obtained from Chief Mike Lasnier, Post Office Box 1021, Squamish, Washington 98392, (360) 598-4334:

Tribal Law Enforcement Information Sharing Initiative: *Concept of Operations*, 2005.

Northwest Association of Tribal Enforcement Officers, *Governance Board Charter*, 2005.

- Tuckman, Bruce, Ph.D., *Forming Storming Norming Performing [Team Development] Model*, 1965, www.businessballs.com/tuckmanformingstormingnormingperforming.htm.
- Varney, G. H., *Building Productive Teams: An Action Guide and Resource Book*, San Francisco: Jossey-Bass Publishers, 1989.

This book offers information that shows how to systematically build a productive team by identifying, understanding, and overcoming the inherent problems that occur in a team's day-to-day work.

Section 6—Establishing a Charter

Through the planning process, the policy development team can ensure production of a concrete, articulated privacy policy within a reasonable time frame. The systematic process of building commitment among team members and key stakeholders to meet a common mission and goal is essential for acceptance of the policy by those most affected by its implementation. Good planning can focus attention on common goals, articulate individual responsibilities, identify individual issues and challenges, and provide a timetable for completing tangible products.



6.1 Components of a Charter

The first step in the planning process should be a team effort to produce a charter—a set of written guidance statements that serve as an overall guide to both the project and to the team. The process of developing these statements is as important as the statements themselves. The process will help to build team trust and serve as a reference for all team members throughout the effort.

The team charter should include guidance statements comparable to a vision statement, mission statement, values statement, and goals and objectives as hierarchical declarations that logically flow from one to the other. Conceptual definitions are as follows:

- **Vision:** A compelling conceptual image of the desired, successful outcome.
- **Mission:** A succinct, comprehensive statement of purpose of an entity, program, subprogram, or project that is consistent with the stated vision.
- **Values:** The core principles and philosophies that describe how an entity conducts itself in carrying out its mission.
- **Goals:** The desired long-term results that, if accomplished, would mean the team has achieved its mission.
- **Objectives:** Specific and measurable targets for accomplishing goals that are usually short-term with a targeted time frame.

6.1.1 Vision Statement

Ideally, most justice entities have an articulated vision statement and/or mission statement. This can serve as the starting point for the project team in developing a vision statement. The vision statement describes a compelling conceptual image of the desired, successful outcome.

For example, GPIQWG adopted the following vision statement:

“To accomplish justice information sharing that promotes the administration of justice and public protection by:

- *Preserving the integrity and quality of information.*
- *Facilitating the sharing of appropriate and relevant information.*
- *Protecting individuals from consequences of inappropriate gathering, use, and release of information.*
- *Permitting appropriate oversight.”*

6.1.2 Mission Statement

If the entity does not have a vision statement but has a mission statement, use the mission statement as a starting point for the project’s mission, narrowly focusing on the specifically assigned responsibility. Mission statements are generally short, preferably no more than a paragraph. The mission statement provides the common statement of purpose among project team members and helps identify the function that the project team is supposed to serve.

The mission statement should not describe strategies or detail how to accomplish the mission but is a statement of the long view of the project team’s resulting effort. A mission statement serves both as an internal document and a public statement to stakeholders and interested persons about the team’s focused efforts to address privacy issues and promote information sharing. The mission statement should:

- Educate.
- Establish expectations and limitations.
- Clarify organizational purposes and foster cooperation.

The following is an example of a mission statement:

“The mission of [name] is the development and implementation of a privacy, civil rights, and civil liberties policy that promotes justice information sharing while protecting individuals, public safety, and privacy.”

Throughout the course of the project team’s development of the privacy policy, frequent reference to the mission statement as a resource can help the team focus on activities that contribute directly to policy development and implementation.

6.1.3 Values Statement

A values statement provides the guiding or defining principle or principles by which the team will operate. It describes the core principles by which the team will be bound as it develops the privacy policy.

Although a values statement is not always necessary, it is recommended that the policy development team engage in some discussion of values because of the nature of the issues. Recognized inherent conflicts among justice system information sharing and privacy protection interests will inevitably lead to a team of stakeholders with many varied perspectives. Development of common values statements helps establish the rules by which the team, with desired differing interests, will work and will build trust among team members that all perspectives will be considered when formulating policy statements.

The following are examples of values statements:

- “We believe victims have a special interest in their privacy.”
- “We demand integrity and ethical behavior by entity employees and users at all times.”
- “We accept our responsibility in the protection of personal privacy.”
- “We recognize crime control and prevention as fundamental law enforcement responsibilities.”

Note, however, that the above are only examples. The process a team experiences in developing such statements, establishing a culture of trust, is as important an outcome as the values statements themselves.

6.1.4 Goals and Objectives

After developing mission and values statements, the next planning tool for the team effort is the identification of clear goals and objectives. Goals and objectives are more specific statements of sought-after outcomes that, when achieved, help the team achieve its mission. Goals are broad, intentional targets that may be intangible and abstract but are more specific than the mission statement. Objectives are more tangible, narrow, and concrete statements of outcomes that typically will be completed within a limited time period.

6.1.4.1 Goals¹⁵

Goals provide a framework for more detailed levels of planning. Goals are more specific than the mission statement but remain general enough to stimulate creativity and innovation.

6.1.4.2 Objectives¹⁶

Objectives are specific and measurable targets for accomplishing goals. While goals provide a general planning framework, objectives are specific, quantifiable, and time-bound statements of desired accomplishments or results. As such, objectives represent intermediate achievements necessary to achieve goals.

The following are examples of goals with associated objectives:

Goal: Increased justice information sharing among identified entities.

Objective: Clearly stated rules for information sharing between entity A and entity B by [date].

Goal: A written privacy policy that is current.

Objective: A stated privacy policy provision that describes the timing and process for review and revision of the policy.

Goal: Executive support for the implementation of the privacy policy.

Objective: An education/marketing plan for entity executives.

While development of these various planning tools will take time, in the end, they contribute to more efficient and effective project team operations. Because all team members participate and present their perspectives and because all team members agree to the final statements, the team charter functions as a valuable resource that keeps the team on target throughout the process.

¹⁵ Anne Seymour, *Strategic Planning Toolkit*, adapted from Office for Victims of Crime, 2004.

¹⁶ Ibid.

6.2 Writing the Charter

After completing the vision, mission, and values statements and the goals and objectives, the team should collect these organizing tools into one document, known as the project charter. The charter will serve as a reference and resource throughout the course of the policy development effort. It should memorialize the current status of the effort and can be amended when things change. There is no hard-and-fast rule that dictates the charter contents or length. The most critical feature of the charter is that it memorializes the planning efforts and agreements of the team members to achieve specific goals and thus serves as an historical record of team plans and activities.

At a minimum, the charter should include an introduction that describes what the charter is about, a section with background information that includes a statement about the authorization or mandate to develop the privacy policy, and a section on membership that includes team member names, as well as a description of member skill sets or special interests. Finally, the charter should reiterate the vision, mission, and values statements and goals and objectives that the team has adopted.

The following is an example of the table of contents of a project charter:

- I. Introduction
- II. Background
- III. Membership
- IV. Mission
- V. Values Statements
- VI. Goals and Associated Objectives

Depending on the nature of the project team and the formality of the assignment to develop a privacy policy, the charter should be presented for approval to the project champion or sponsor once all project team members have adopted it.

6.3 Resources

- Foundation Center, "Develop Vision and Mission Statements," <http://foundationcenter.org/getstarted/tutorials/establish/statements.html>.
- Global Advisory Committee (GAC), *Charter*, 2002, www.it.ojp.gov/GAC_Charter.
- Global, *Guiding Principles and Strategic Vision of the Global Justice Information Sharing Initiative*, Mission Statement, page 4, September 2004, http://it.ojp.gov/documents/200409_GAC_Strategic_Plan.pdf.
- Global, *Guiding Principles and Strategic Vision of the Global Justice Information Sharing Initiative*, Vision Statement, page 3, September 2004, http://it.ojp.gov/documents/200409_GAC_Strategic_Plan.pdf.
- GPIQWG, Vision Statement, http://it.ojp.gov/topic.jsp?topic_id=55#Vision.
- GPIQWG, Mission Statement, http://it.ojp.gov/topic.jsp?topic_id=55#Mission.
- Melton, A. P., and S. Wall, *Integrated Justice Systems in American Indian Communities Planning Series: Preliminary Planning for Justice Integration in Tribal Communities*, 2004, www.aidainc.net/Publications/Planning_IJS.pdf.
- Radtke, Janel M., "How to Write a Mission Statement," 1998, www.tgci.com/magazine/How%20to%20Write%20a%20Mission%20Statement.pdf.

Section 7—Understanding Information Exchanges



If the entity has followed the guidance provided thus far, the groundwork has been set—a project champion has been identified, a project team leader and project team members have been appointed, some sense of resource needs (or resource limitations) have been estimated, and a charter has been drafted that lays out the project team’s guidance statements (vision, mission, and values statements and goals and objectives). Now the work of the team begins on the substantive activities that will provide the basis for the privacy protections. Some preliminary analysis of the scope of the project will help to assure the team that development of a policy is not impossible.

Prior to the legal analysis, described in Section 8, it is important to fully understand the information exchanges to which the privacy policy will apply and then perform a Privacy Impact Assessment to examine the privacy implications for these exchanges.

7.1 Understanding Information Exchanges

Understanding the relevant information exchanges—that is, determining what PII the entity collects, manages, and protects—will define the scope of the project and guide the policy development process because the project team will limit its development of privacy policy to information that it collects, exchanges, or controls.

Understanding information exchanges or flows not only distinguishes information that should be the subject of the policy development efforts but also pinpoints where that information is along the continuum of a justice process. Highlighting the decision points at which privacy becomes an issue for information collection, use, and dissemination automatically places reasonable limits on the process of developing a policy.

Begin the process with the project team by asking questions about the information the entity gathers from within and outside its organizational “walls” that it needs in order to conduct usual business activities. This inquiry can be broken down into approximately four categories:

1. Information collection (creation and receipt)
2. Information maintenance

3. Information use (access and dissemination)

4. Information retention and disposition

The questions to be answered are as follows: (As you ask these questions, also consider what privacy laws, policies, or restrictions apply at each stage of the flow of information.)

1. Information Collection (Creation and Receipt)

- What personally identifiable information does my entity collect?
- Why is the information collected?
- What is the source of the information? Where do we get the information?
- Are there any applicable laws that place restrictions on the type of information collected and manner in which it is collected?
- Who within the entity collects the information?
- How is the information gathered? What methods are used?
- Who is responsible for the identification and collection of new data sets?
- How is the information captured (e.g., downloaded from the source's site, e-mail from the source)?

2. Information Maintenance

- What personally identifiable information is maintained by the entity?
- How is the information stored—in paper form or searchable electronic form?
- Who is responsible for ensuring the accuracy of the information collected or gathered?
- Who is responsible for updating and aging out the information?

3. Information Use (Access and Dissemination)

- Who within the entity uses the information?
- Who within the entity controls access to the information?
- How does the entity authenticate users within the entity?
- For what purpose does the entity use the information?
- Are all uses consistent with the purpose for which the information was collected?
- Who outside the entity (i.e., nonpersonnel) has access to the information (e.g., Web access through a criminal justice information sharing effort)?
- How does the entity authenticate users (both personnel and nonpersonnel) who access the information from outside the entity?
- With whom does the entity share the information?
- Why is it shared?
- How is it shared?
- Who authorizes the sharing or dissemination of the information?
- Is the entity required to notify those who have accessed or received information from the entity when it subsequently discovers there were errors in the information when it was shared or accessed?

4. Information Retention and Disposition

- Who is responsible for developing and implementing information management and retention issues?
- What are the records retention policies for the entity?

- How long can the entity keep information?
- When must the entity purge and destroy the information?
- Are there policies requiring the entity to review information for possible purging when updated or more current information becomes known?
- What software or systems are used to manage the information?
- Is the entity required to notify those who have accessed information or with whom it has been shared when it is subsequently purged or updated?
- Does the entity have to keep a record of what information has been destroyed or purged?
- Who is responsible for expunging the information pursuant to court order? Are there policies in place that govern this process?

There are various tools available to assist with understanding information exchanges and in answering these essential process questions. The team members must select the methods for this data collection effort about information flow—focus groups, interviews, or technical tools. The team should investigate whether any mapping tools have been used for other purposes that could be amended to meet the needs of the team.

An information flow map, for example, will reveal those decision points where different privacy protections attach. Varying laws may apply to information at distinct stages of the justice process. For example, a law enforcement officer may receive a tip that a crime has been committed. He may investigate the tip and make an arrest that ultimately leads to a conviction, or the charges may be dismissed. At each stage of the process, there will be some collection and communication of PII about the alleged offender, victims, and witnesses. The privacy restrictions and protections may differ for this information depending upon the process stage and the individuals involved.

Once an information flow model is created for an entity system or an interentity information exchange, the model can then be reused for other related systems. Thus, an information flow model for the criminal justice system may need only a few additions and revisions to apply to the juvenile justice system. Adding social services interactions with the court, attorneys, or other advocates, along with the particulars of the postdisposition organizations, may be the only needed additions to capture and understand the entire flow of information.

Frequently, systems developers of case management or records management systems map information flow during the design stage. Determine whether information flow maps already exist with respect to the system in question. With an existing information flow map, the only additional step for assessing privacy implications may be the analysis of changes to information privacy at each information exchange point.

Ask these critical questions: What is the PII? What is its source? Who has or wants access to it? To whom is it communicated? How is it communicated, and for what purpose is it communicated? Finally, and most important, what privacy laws, policies, or restrictions apply at each stage of the process?

7.1.1 Tools to Assist With Understanding the Flow of Information

The following is a brief listing of tools that may be useful to an entity in understanding and illustrating information exchanges.

7.1.1.1 Criminal Justice System Flowchart

DOJ's Bureau of Justice Statistics (BJS) has produced a useful flowchart that depicts the sequence of events in the criminal justice system. This chart is included in Appendix B of this guide and is also available online at <http://bjs.ojp.usdoj.gov/content/justsys.cfm>. BJS updated this version from the original chart prepared by the President's Commission on Law Enforcement and the Administration of Justice in 1967. The chart portrays the most common sequence of events in the criminal and juvenile justice systems in response to serious criminal behavior, including entry into the criminal justice system, prosecution and pretrial services, adjudication, sentencing and sanctions, and corrections.

7.1.1.2 *Justice Information Privacy Guideline*¹⁷

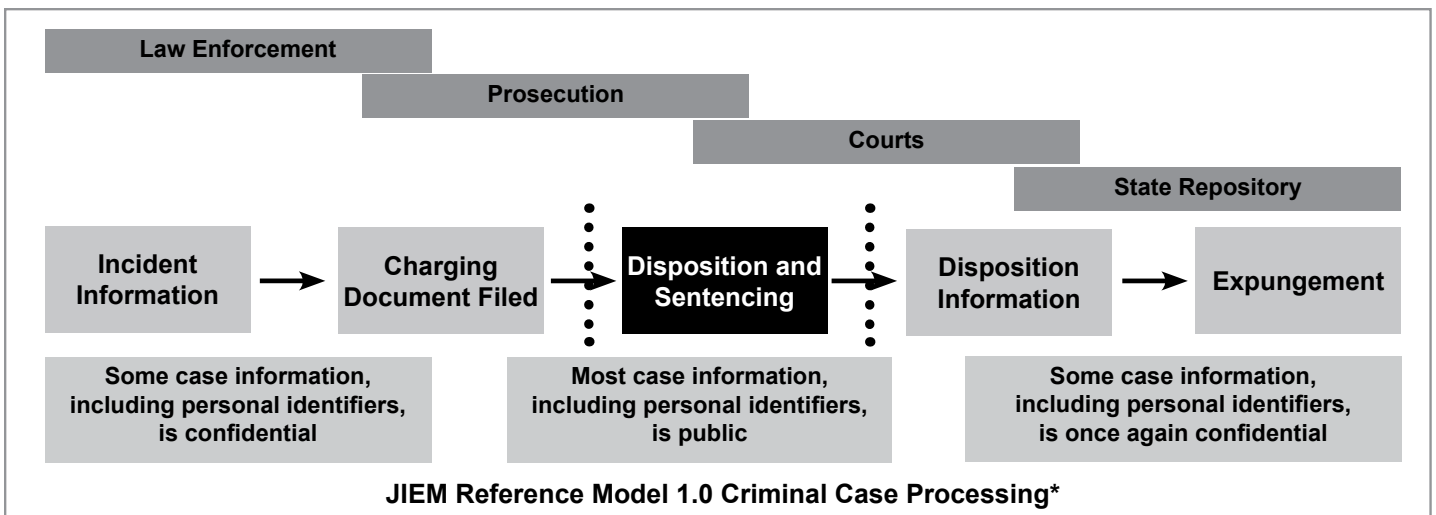
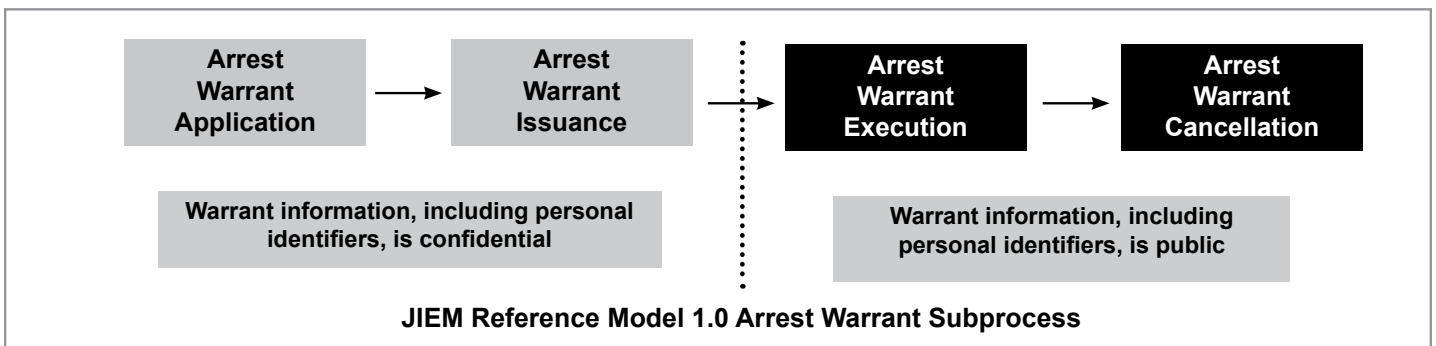
Developed by the National Criminal Justice Association, this 2002 guide provides background information on the development and history of privacy policies, as well as specific tools for Mapping Information Flows (Chapter 6).

7.1.1.3 Justice Information Exchange Model (JIEM)

Developed by SEARCH, The National Consortium for Justice Information and Statistics, the Justice Information Exchange Model (JIEM)¹⁸ is a useful tool in planning and implementing justice integration projects. The JIEM is a conceptual framework that defines the dimensions of information exchange, a research and planning methodology for modeling the operational dynamics of this information exchange, and a Web-based software application—the JIEM Modeling Tool—that enables data collection, analysis, and reporting by users and researchers. Although originally designed to aid the systems development process, the JIEM tool is also valuable for breaking down criminal justice processes into key decision points and identifying critical points where the justice community shares and accesses information electronically.

The following diagrams are examples of a high-level depiction of a JIEM functional flow, illustrating how privacy concerns may change around a set of information as the information moves through various processes.

JIEM Reference Model 1.0



*This illustration depicts a partial model. It does not, for example, include as part of the information sharing community the defense, corrections, prerelease, and postdisposition treatment entities or other private government participants in the justice arena.

17 National Criminal Justice Association (NCJA), *Justice Information Privacy Guideline: Developing, Drafting and Assessing Privacy Policy for Justice Information Systems*, September 2002, www.ncja.org/NCJA/Policies_and_Practices/Justice_Information_Privacy_Guideline/NCJA/Navigation/PoliciesPractices/JusticeInformationPrivacyGuideline/Information_Privacy_Guideline.aspx?hkey=d80450ef-9e42-4f05-bb10-1f23222b34ee.

18 SEARCH, The National Consortium for Justice Information and Statistics, Justice Information Exchange Model (JIEM), www.search.org/programs/info/jiem.asp.

The Justice Information Exchange Model has proved to be valuable in analyzing the flow of criminal justice information and in modeling complex business processes. For more information on the JIEM, refer to www.search.org/programs/info/jiem.

7.1.1.4 Information Life Cycle¹⁹

The information life cycle is a simple framework for illustrating the flow of information through a justice event. Creating a list of the information generated by the business processes within the organization is a good starting point for an agency to understand what information the agency creates, captures, stores, maintains, uses, shares, and disposes of or destroys. These may be incident reports, presentencing reports, litigation case files, investigative files, disposition reports, or criminal history reports.

Information Life Cycle			
Justice Event or Process:			
Life Cycle Phases	Components of Each Phase		
	Roles and Responsibilities	Policies and Procedures	Information Technology
Creation and Receipt			
Maintenance			
Use			
Disposition			

Using a table such as the one shown above, an entity can break down the individual report into phases and components of the information life cycle. This task will illustrate the flow of information from creation and receipt to maintenance, use, and disposition and destruction. Identify components of each phase: roles and responsibilities, policies and procedures, and information technology. This framework will help organize the flow of information to make it easier to apply core dimensions and to determine which contextual dimensions may apply to each phase and component of the justice event. For more information and to see an example of a completed Information Life Cycle, refer to Section V, Figure 2, of the *Global Information Quality Program Guide*, available at www.it.ojp.gov/IQ_Resources.

7.2 Privacy Impact Assessment (PIA)²⁰

The availability of information, from personal information to public information, is made all the easier today due to technological changes in computers, digitized networks, Internet access, and the creation of new information products. The E-Government Act of 2002²¹ recognized that these advances also have important ramifications for the protection of personal information contained in government records and systems.

Understanding entity privacy risks is critical to the development of a privacy policy that establishes how an agency collects, maintains, and shares agency justice information. A Privacy Impact Assessment (PIA) is a

¹⁹ U.S. Department of Justice, Global Justice Information Sharing Initiative's *Information Quality Program Guide*, Section IV, Identify Justice Events and Information Products, and Section V, Analysis—IQ Dimensions and the Information Life Cycle, B. Information Life Cycle, January 2010, www.it.ojp.gov/IQ_Resources.

²⁰ U.S. Department of Justice, Global Justice Information Sharing Initiative's *Guide to Conducting Privacy Impact Assessments for State, Local, and Tribal Justice Entities*, www.it.ojp.gov/pia_guide.

²¹ E-Government Act of 2002, PL 107-347, December 17, 2002. This act requires covered agencies to conduct a Privacy Impact Assessment (PIA) before developing or procuring information technology systems or projects that collect, maintain, or disseminate information in identifiable form, from or about members of the public. *In general, PIAs are required to be performed and updated, as necessary, when a system change creates new privacy risks.* See OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, www.whitehouse.gov/omb/memoranda/m03-22.html.

comprehensive process designed to assist organizations in determining the effects of information services and sharing initiatives on individual privacy. Similar to a risk management approach, the fundamental components include project analysis, data analysis, privacy analysis, and a Privacy Impact Assessment report. PIAs analyze and describe:

- The information that is to be collected.
- Why the information is being collected.
- The intended use of the information.
- With whom the information will be shared.
- What opportunities individuals will have to provide information or to consent to particular uses of the information.
- How information will be secured.
- Whether a system of records is being created under the privacy policy.

A PIA allows justice practitioners to examine the privacy implications of their information systems and information sharing collaborations so they can design and implement policies and procedures to address vulnerabilities and protect PII and other personal, sensitive information to ensure that it is not improperly collected or distributed.

7.2.1 PIA Template

Privacy policies emerge as a result of the analysis performed during the Privacy Impact Assessment (PIA) process. In addition to an overview of the PIA process, the ***Guide to Conducting Privacy Impact Assessments for State, Local, and Tribal Justice Entities*** (www.it.ojp.gov/pia_guide) contains a template that leads policy developers through a series of appropriate PIA questions that evaluate the process through which PII is collected, stored, protected, shared, and managed. The PIA questions are designed to reflect the same policy concepts as those recommended in this Privacy Guide.

7.3 Resources

- *Global Guide to Conducting Privacy Impact Assessments for State, Local, and Tribal Justice Entities*, www.it.ojp.gov/pia_guide.
- *Global Information Quality Program Guide*, www.it.ojp.gov/IQ_Resources.
- Justice Information Exchange Model (JIEM), SEARCH, The National Consortium for Justice Information and Statistics, www.search.org/programs/info/jiem.
- National Criminal Justice Association (NCJA), *Justice Information Privacy Guideline: Developing, Drafting and Assessing Privacy Policy for Justice Information Systems*, Chapter 3, September 2002, www.ncja.org/Content/NavigationMenu/PoliciesPractices/JusticeInformationPrivacyGuidelines/default.htm.
- U.S. Department of Justice, Bureau of Justice Statistics, Criminal Justice System Flowchart, <http://bjs.ojp.usdoj.gov/content/justsys.cfm>.
- U.S. Department of Justice, Privacy and Civil Liberties Office, *Privacy Impact Assessments*, www.usdoj.gov/pclo/pia.htm.

Section 8—Performing the Legal Analysis



Once an entity understands the information exchanges to which the policy will apply and examines the privacy implications of those exchanges through a PIA (refer to Section 7), the next step is to perform a legal and policy analysis of existing authority and constraints regarding the collection and use of the set of information exchanges identified. Also part of this process is identifying the unresolved critical issues and gaps that will require entity policymaking, entity rule making, or legislation. Simply put, a privacy policy should enable entities to comply with the law.

The project team or individual assigned to this task must conduct an analysis of local, state, tribal, and federal laws and identify those that apply to the information the entity handles. This analysis will provide guidance to the entity about what information may be collected, what information may not be collected, the manner in which the information can or cannot be collected, and with whom it may be shared. This legal analysis will also identify gaps where there is no law to guide the policy or where there are conflicts in law and practice that need to be reconciled before drafting a policy. The objective of the legal analysis is to produce a policy that complies with both the letter and the intent of all applicable local, state, tribal, and federal laws.

The legal analysis should be part of the policy development process at the planning stage, not postponed until project operations are under way. It is much easier to integrate access, privacy, and disclosure capabilities into a project during the design phase than it is to retrofit. Additionally, prior to completion of the privacy policy, it will be important to include the results of this legal analysis (a list of citations to legal authority) within the provisions of the privacy policy, where appropriate, to illustrate to entity personnel, participating agency personnel, and the general public the legal authority under which the entity has shaped its policies.

8.1 Approach to the Legal Analysis

One of the keys to conducting an efficient legal analysis is to look at all of the variables that could influence policy development. Analyzing these variables will help establish the scope of the legal analysis. For example, for tribal groups, it is important to remember that policy analysis conducted by state and federal entities is often not applicable to Indian country jurisdictions. Therefore, it is essential for tribal groups to identify the people who can provide both culturally relevant and appropriate analysis, as well as legally sound analysis, based on tribal and/or indigenous law. For other task teams, similar parameters may exist.

The approach and suggestions provided in Section 8.2.1, Suggestions for Approaching the Legal Analysis, cover a wide range of topics. Note that all privacy policies may not necessarily need to address all of the legal issues identified. By first defining the scope of the privacy policy (the information and information exchanges identified in Section 7), the project team can best determine which of the sources listed in Section 8.2.2, Potential Sources of Legal Authority and Limitations, are relevant to the policy.

The range of the legal analysis will depend upon the scope of the project. Decide which entity or entity representative will perform the legal analysis (for example, the entity's legal counsel or, perhaps, if a state agency, the office of the district attorney). The project team, on its own, may not be responsible for the full legal analysis. Look for assistance from the legal departments of the various entities represented on the team. Help may also be available from other entities, such as peer agencies that may have already developed a privacy policy. Citations from their legal analysis may be included or leveraged within the policy. Tribal, state, and national groups may have already conducted a similar legal analysis; as such, help may be available through the tribe's legal counsel or tribal attorney's office.

The legal analysis is particularly important when the project involves Indian tribes. A growing number of tribes are participating in multitribal justice information sharing initiatives. Additionally, most tribes have a legal department, office, or legal counsel that should be enlisted to provide an overview of applicable tribal laws.

There is no universal privacy policy that an entity can simply adopt as an unmodified template. For each project, the entity must examine applicable law to develop a policy that is compliant and consistent with those laws, including local or tribal law, and the expectations of funders, users, and the public.

8.2 Focusing the Legal Analysis

8.2.1 Suggestions for Approaching the Legal Analysis

The initial objective of the legal analysis is to identify the key legal issues facing the entity and the entity's privacy protection efforts. This step is eased if the project team has first conducted the information flow analysis and defined the scope of the project, as discussed in the previous chapter of this guide.

First, begin with work that has already been done. The entity probably has existing policies and common practices in place that are pertinent to the team's mission. These, for example, may be scattered in policy manuals, concept of operations, standard operating procedures, bulletins, directives, and memoranda. Gather, review, and organize these documents in a way that exposes the gaps or inconsistencies, if any, with applicable law.

Next, find and leverage the work of others who have already completed some of the legal analysis within the state, for the local tribe, or nationally.

For tribes in particular, legal analysis assistance may be available from organizations such as the National Congress of American Indians (NCAI).²² The NCAI often conducts policy analysis on overarching issues impacting tribes, such as those dealing with privacy and security, related to information sharing. Tribal groups should look for similar intertribal projects and tribal associations, such as the Northwest Association of Tribal Law Enforcement Officers and others.

The next section of the guide identifies and provides references to a number of existing resources of relevant legal analysis.

8.2.2 Potential Sources of Legal Authority and Limitations

Identify all possible local, state, tribal, and federal laws and policies that apply to the PII the entity collects, receives, stores, maintains, accesses, and shares. These laws may have provisions governing the collection, use, sharing, or retention of certain types of information or information about certain classes of individuals. Examples of the types of laws the project team may need to examine include:

22 National Congress of American Indians (NCAI), www.ncai.org.

- Case law—federal and state.
- Constitutions—state, tribal, and federal.
- Court procedural and practice rules.
- Descriptions of tribal customary law.
- Executive orders.
- Family relations law, in particular child custody and domestic violence.
- Federal statutes and regulations (some of these are included in Appendix C.3).
- Laws regarding a criminal history repository.
- Laws regarding a criminal intelligence system.
- Laws regarding an integrated justice information system.
- Laws regarding civil commitments of individuals who pose a threat to themselves or others because of mental illness.
- Laws regarding civil harassment, restraining, and stay-away orders.
- Laws regarding juveniles, in particular regarding confidentiality of proceedings.
- Laws regarding medical records and information.
- Local ordinances.
- Open-meeting laws as they affect the entity or the governing body of a justice information system.
- Professional codes of ethics.
- Public records acts, in particular, regarding justice system records and information.
- State Attorneys General opinions.
- State statutes and regulations.
- Treaties.
- Tribal court rules.
- Tribal ordinances.
- Tribal resolutions.

Refer to the list of more specific legal topics in Section 8.3.2, Specific Laws to Examine. The following discussion will help the project team simplify the legal analysis process and reduce the number of legal sources that need to be examined.

8.2.2.1 Federal Laws Relevant to Seeking, Retaining, and Disseminating Justice Information

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

8.2.2.2 State, Municipal, Local, and Other Sources

In addition to the U.S. Constitution and applicable federal laws, SLT agencies may also be subject to a variety of state, regional, local, and tribal laws that need to be identified and reviewed to determine their impact on agency operations and privacy policies (see Section 8.3.2). Applicable laws may include the state constitution (which may provide enhanced protections of privacy and civil liberties over and above those required by the U.S. Constitution), executive orders, public records laws, sunshine laws, data breach notification laws that apply to public agencies, and agency regulations and policies. With regard to local ordinances and tribal laws, these may be identified through contact with local and tribal governing agencies.

8.2.3 Particular Events and Actions

The process of identifying laws that are applicable to the privacy policy development project requires a context. One approach is to think in terms of the events, transactions, and information exchanges about which information will be captured by the entity and which are affected by the policy. The legal analysis can proceed by identifying laws that govern these events, transactions, or exchanges. These should be examined to determine whether there are restrictions, prohibitions, standards of behavior, or specific legal authority for collecting, storing, using, sharing, or disclosing information of the type identified by the project. The following list describes typical events, transactions, and information exchanges that might be involved in this project:

- Arrests.
- Arrest warrants.
- Convictions—any distinctions based on seriousness of crime.
- Disposition.
- Domestic violence, civil harassment, and stay-away orders.
- Enforcement of planning, zoning, environmental, and similar laws.
- Expungement.
- Informants.
- Information generated during a trial.
- Interrogation.
- Investigation—existence, work products.
- Laboratory or forensic testing or analysis.
- Law enforcement contacts—in particular, traffic stops.
- Lineups.
- Officer logs.
- Officer reports—field reports, formal reports, supplemental reports.
- Other events, transactions, or activities revealed in the project team’s information exchange analysis.
- Parole—in particular, terms and conditions.
- Probation—in particular, terms and conditions.
- Retention.
- Search warrants.

- Sentencing information, including programs providing alternatives to incarceration.
- Surveillance, including pen registers and packet sniffers.
- Treatment programs, including those imposed by problem-solving courts such as drug courts.
- Trial activities.
- Victim advocate logs.

8.2.4 Information Related to a Specific Person

Frequently, laws that are relevant to the development of a privacy policy are triggered only if the policy covers information that relates to a specific, identifiable person (e.g., PII). Expectations about privacy and laws that respond to these expectations often address only the collection and, more important, sharing of PII (refer to Section 4.1.1 and Appendix C.2, Glossary of Terms and Definitions, for more information on PII). Therefore, the examination of laws that might apply to a privacy policy depends on what types of PII are to be gathered, what PII will be shared by the entity, and with whom the information will be shared. Information that does not constitute PII will generally have far fewer limitations, both in terms of gathering and sharing, than will PII.

8.2.5 Information Related to Groups

Organizations and groups have constitutional rights of their own to assert under some circumstances. Even when they do not, the collection, use, maintenance, and sharing of information about them may raise privacy, civil rights, and civil liberties concerns about the individuals who are members of or who are associated with the organization or group. These individuals may be chilled in the exercise of their constitutional rights (e.g., discouraged from exercising) by allegations about the activities of the organization or group (for example, that it may be engaging in criminal activity).

Beyond what the law mandates, law enforcement agencies can address these concerns to some extent by requiring a valid law enforcement purpose (e.g., criminal nexus, public safety concern) in order to gather information about an identifiable individual, an organization, or a group. Policies can provide that if there is no evidence of involvement in criminal activity identified under agency investigative guidelines, then the law enforcement activity must cease within a reasonable period of time and the investigative file should be destroyed because there is no valid law enforcement purpose for its retention. Retention of such official files would constitute the maintenance of inappropriate “dossiers” on the individual, organization, or group. Having a legitimate law enforcement purpose, however, does not always, or alone, validate governmental conduct that intrudes upon individual rights.

Also, some laws, regulations, and privacy policies expressly extend protections to organizations, both formal (such as a corporation or association) and informal (such as a gang), that have a recognizable structure. Code of Federal Regulations Title 28, Part 23 (28 CFR Part 23), for example, protects information about organizations, because if an organization is determined to be a criminal subject, individuals who are members of or associated with that organization may be tainted by the documentation of its alleged criminal activity.

Governmental agencies must also exercise caution in drafting and disseminating analytical products. The inclusion of an organization or group in a report may implicate their rights of freedom of expression and association under the First Amendment to the Constitution, regardless of whether they are harmed (e.g., drop in membership or subjected to public derision) as a result of the report. Moreover, if this information is entered into an information system and is later used to deny members of the organization or group a benefit, right, or privilege, then due process rights may also be implicated. Consequently, law enforcement should avoid making sweeping generalizations about the propensity for or involvement of organizations and groups to engage in criminal activity. Generalizations, unsupported by articulable facts and circumstances, fail to convey useful information because they are by their nature vague and overly broad and thus are likely to include the lawful activities of innocent individuals. Finally, law enforcement should proceed cautiously when attributing the criminal activities of an individual to an organization or group as a whole, absent information that the organization or group publicly claims responsibility or is, itself, a criminal enterprise.

8.3 Performing the Legal Analysis

8.3.1 Principles

The following approach tracks the typical steps in the collection and use of information by the justice system. It begins with the collection of the information, addressing what can be collected, how it can be collected, and information quality. The approach then addresses the use, sharing, and dissemination of the information. Included is Section 8.3.1.4, Provisions Relevant to Individuals' Access to Information About Themselves, which addresses access by an individual to information that is about that person. Next are the issues relating to retention and purging of information. Finally, there are subsections on entity transparency and accountability regarding the privacy policy and entity operations.

For each of the stages of the information gathering and use process, there is a listing of the potential subjects to be researched. The research should focus on what authority, limitations, or prohibitions are contained in law governing the gathering, maintenance, use, and sharing of information. To provide a general background, the discussion of each stage begins with a summary of the related Organisation for Economic Co-operation and Development (OECD) Fair Information Principles (FIPs)—Basic Principles.²³ Although the FIPs were developed around commercial transactions and the transborder exchange of information, they do provide a straightforward description of the underlying principles and 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.

8.3.1.1 Collection of Information

The information collection stage concerns not only the act of collecting information but also the means of collection. The FIPs Collection Limitation Principle²⁴ requires entities to review both what information they collect and how they collect it. The intent is to avoid unnecessary collection of information and to ensure that only lawful and fair means are used to collect information. In the justice context, the legal analysis should answer the following questions:

- Are there legal provisions specifying what information can or cannot be collected by the entity/project based on its role and scope?
- Are there laws that prohibit the gathering of certain types of information—for example, information that relates to the exercise of free speech, free association, or religious freedom—or prohibit gathering of information that involves racial or a similar basis of discrimination?
- Are there laws that specify a standard for the gathering of information, such as the requirements for obtaining a warrant for search and seizure?
- Are there laws that specify limits on what methods can be used to collect information?
- Are there laws controlling what information can be obtained from third-party, nonpublic information sources? What about concerning the means the third party used to gather the information?
- What are the requirements, if any, for uniquely identifying an individual who seeks to add information to the entity/project's database; that is, what are the means of authenticating users?

²³ Organisation for Economic Co-operation and Development (OECD), Fair Information Principles (FIPs)—Basic Principles include Purpose Specification Principle, Collection Limitation Principle, Data Quality Principle, Use Limitation Principle, Security Safeguards Principle, Openness Principle, Individual Participation Principle, and Accountability Principle.

²⁴ FIPs Collection Limitation Principle: There should be limits to the collection of personal data, and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

8.3.1.2 Information Quality Relative to Collection and Maintenance of Information

In order to be relevant and useful, the information collected must be of high quality. The FIPs Data Quality Principle²⁵ states that the PII gathered should be relevant to the purpose for which it was gathered, and it should be accurate, complete, meaningful, and current. This not only protects individuals, it is necessary for the proper and effective operation of the entity and minimizes waste and misuse of entity resources. Refer to Appendix C.1, SLT Policy Development Template, Section G, Information Quality Assurance, for recommended policy provisions designed to address these issues. For more guidance on information quality, refer to the Global *Information Quality Program Guide*, available at www.it.ojp.gov/IQ_Resources.

8.3.1.3 Sharing and Dissemination of Information—Public Access

One of the main purposes of gathering information is to share it with others in the justice system so that the system better accomplishes its mission of ensuring justice and protecting public safety. However, there must be limits on the sharing of information—with whom and under what circumstances it may be shared. The FIPs Use Limitation Principle²⁶ asserts that the information gathered should be shared or used only for the purpose for which it was gathered. This is the key to protecting individual privacy. Relevant sharing and dissemination questions for the legal analysis include:

1. Are there legal provisions regarding sharing of information? With whom can information be shared or not shared?
2. What do the state constitution, statutes, and case law interpreting the provisions say about openness of entity records and the extent of public access to the information?
3. Is there a law enforcement exception to this public access? If so, how broad is it? To what classes of information does the exception apply?
4. What exceptions exist for specific types of information (for example, arrests, dispositions, or convictions)?
5. What legal exceptions are there regarding specific uses of information? Are there legal provisions with regard to providing information for background checks, preemployment checks, or other noncriminal justice uses? Has certain information been received that is subject to restrictions concerning further dissemination?
6. Are the public access rules for court records more open than for other entities? When do these rules begin to apply? When is information from other justice system entities introduced into the court record in a case?
7. Are there provisions allowing selling of information to information brokers or third parties? Are there specific categories or types of information for which such bulk transfer of information is permitted or prohibited? Can downstream or third-party use of the information given to information brokers be controlled?
8. What are the requirements for uniquely identifying an individual who seeks access to the information maintained by the entity; that is, what are the means of authenticating users? What are the means of keeping a historical record of the persons or entities with which information has been shared?

²⁵ FIPs Data Quality Principle: Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete, and kept up to date.

²⁶ FIPs Use Limitation Principle: Personal data should not be disclosed, made available, or otherwise be used for purposes other than those specified in accordance with [the Purpose Specification Principle] except (a) with the consent of the data subject or (b) by the authority of law.

8.3.1.4 Provisions Relevant to Individuals' Access to Information About Themselves

The FIPs Individual Participation Principle²⁷ focuses on individuals and their access to information about themselves. It requires that individuals be able to determine whether there is information about themselves, to find out what that information is, and to be able to challenge its quality. Relevant sharing and dissemination questions regarding information about an individual for the legal analysis include:

1. Are there applicable legal requirements regarding notice to individuals of the existence of information about themselves in entity records? If individuals make inquiries, must they be told about information gathered about them?
2. Are there applicable legal requirements regarding individuals' access to information about themselves in the entity records? If confirmation or access is denied, must the individual be informed as to the basis for the denial?
3. Are there applicable legal requirements regarding individuals' right to challenge information about themselves as to its accuracy, completeness, or context?
4. Is there a right of privacy in the state or tribal constitution? How have the courts interpreted this in the justice context?
5. Is there a law establishing a cause of action for invasion of privacy, or is there a constitutional provision that is self-executing? Under what circumstances might it apply in the justice context? Does the entity or project have immunity as a governmental entity?
6. Relative to tribal entities, is there a right to privacy in the tribal constitution, organic documents, tribal customary law, or tribal ordinances? If yes, what are the possible privacy conflicts? What are the remedies for violating tribal privacy laws and/or regulations? Has the tribal court interpreted the Indian Civil Rights Act to include or respect a right to privacy defined by tribal custom or law? Has the tribe established a process to implement any rights to privacy?

8.3.1.5 Information and Record Retention and Destruction

One aspect of information quality is currency—a continuing business need for the information. The entity should have a business records retention policy based on need. There may be local, state, or federal records acts that dictate management of records and their disposition. Records retention and disposition policies support efficient use of public resources by avoiding costs of maintaining and sorting through stale or irrelevant information. Relevant records retention and disposition questions for the legal analysis include:

1. Are there applicable legal provisions regarding records retention and disposition? Must information be kept for a certain period of time or destroyed or transferred after a certain period?
2. What are disposition requirements? Destruction? Transfer? Expungement?
3. Should anyone's permission be obtained prior to disposition of the records?
4. Should anyone be notified before disposition occurs?

27 As stated in the FIPs Individual Participation Principle, an individual should have the right:

- (a) To obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him.
- (b) To have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him.
- (c) To be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial.
- (d) To challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed, or amended.

8.3.1.6 Entity or Project Transparency

Part of the integrity and legitimacy of the entity and the project is derived from the openness about the existence and nature of the project. The FIPs Openness Principle²⁸ requires that entities provide notice about how they collect, maintain, and disseminate information. In addition, ongoing public expectation has fostered an entity best practice of posting the entity's privacy policy on a publicly available Web site and including, within the policy or online, contact information for questions. Further, involving members of the community in the privacy policy effort at the outset or as part of a public review or vetting period supports the entity's mission of transparency. An example of community involvement is the Building Communities of Trust Initiative, discussed further in Section 10.3.1.

Relevant questions for the legal analysis regarding entity or project transparency include:

1. Are there legal requirements that policies or other documentation of the entity's project be made available to the public? If not, consider public expectation and the commonly accepted practice of providing the privacy policy online.
2. Are the provisions of open-meeting laws applicable to the entity or the governing board of the project? Are there exceptions in the laws for specific meetings or types of deliberative processes?

8.3.1.7 Accountability and Enforcement

A good privacy policy is only as good as its implementation. The FIPs Accountability Principle²⁹ requires an entity to have the means to oversee and enforce its policies regarding the collection, use, and sharing of information. Relevant questions for the legal analysis regarding accountability include:

1. Are there legal requirements regarding audits of the information collected and maintained by the entity?
2. What governmental liability or immunity might the entity or project have regarding:
 - Improper collection of information.
 - Improper disclosure of information.
 - Maintaining information the entity knew or should have known to be incorrect.
 - Not disposing of records, as and when required.
3. Are there legal provisions for sanctions, penalties, or other remedies for unauthorized release or use of information?
4. What sanctions, penalties, or remedies, if any, are specified for failure of the entity to comply with open-meeting laws?
5. Are there legal requirements that entity personnel or users receive minimal training? Do the requirements identify training subjects, such as records management, privacy, civil rights, civil liberties, and information quality?

8.3.2 Specific Laws to Examine

The following is a list of specific laws that may apply to the local jurisdiction or state entity and will serve as a checklist for the policy development effort. Not all of these may apply to this project, whereas others not listed may significantly affect the project. The intent of providing the list is to help the project

²⁸ FIPs Openness Principle: There should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data and the main purposes of their use, as well as the identity and usual residence of the data controller.

²⁹ FIPs Accountability Principle: A data controller should be accountable for complying with measures that give effect to the principles stated above.

team avoid missing any important laws. Review this list with the project team and legal advisors to determine which laws need to be examined more closely, given the project. For synopses of primary federal laws an agency should review and, when appropriate, cite within the privacy policy, refer to Appendix C.3 Federal Laws Relevant to Seeking, Retaining, and Disseminating Justice Information.

1. Federal laws and regulations:

(Refer to Section 8.6, Resources, and Appendix C.3 for cited references.)

- Code of Federal Regulations (CFR) Title 28 (28 CFR)—Judicial Administration, Chapter 1—U.S. Department of Justice, Parts 20, 22, 23, and 46.
- Computer Matching and Privacy Act of 1988, 5 U.S.C. § 552a(a), United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a(a); see also Office of Management and Budget, Memorandum M-01-05, “Guidance on Interagency Sharing of Personal Data—Protecting Personal Privacy,” December 20, 2000.
- Criminal History Records Exchanged for Noncriminal Justice Purposes, 42 U.S.C. § 14611, United States Code, Title 42, Chapter 140, Subchapter II, § 14611.
- Disposal of Consumer Report Information and Records, 16 CFR Part 682, Code of Federal Regulations, Title 16, Chapter I, Part 682.
- Driver’s Privacy Protection Act of 1994.
- Electronic Communications Privacy Act of 1986.
- Fair Credit Reporting Act of 1970.
- Federal Records Act, 44 U.S.C. § 3301, United States Code, Title 44, Chapter 33, § 3301.
- Federal Trade Commission Act of 1914.
- Freedom of Information Act of 1974.
- Health Insurance Portability and Accountability Act (HIPAA) of 1996.
- Indian Civil Rights Act of 1968, 25 U.S.C. § 1301, United States Code, Title 25, Chapter 15, Subchapter I, § 1301.
- National Association of State Chief Information Officers’ (NASCIO) Compendium of Federal Laws, pp. 84–86.
- National Child Protection Act of 1993, Public Law 103-209 (December 20, 1993), 107 Stat. 2490.
- National Crime Prevention and Privacy Compact, 42 U.S.C. § 14616, United States Code, Title 42, Chapter 140, Subchapter II, § 14616.
- 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.
- Privacy Act of 1974.
- Privacy of Consumer Financial Information, 16 CFR Part 313, Code of Federal Regulations, Title 16, Chapter I, Part 313.
- Privacy Protection Act of 1980.
- Protection of Sensitive Agency Information, Office of Management and Budget (OMB) Memorandum M-06-16 (June 2006).
- Right to Financial Privacy Act of 1978.
- Safeguarding Against and Responding to the Breach of Personally Identifiable Information, OMB Memorandum M-07-16 (May 2007).
- Safeguarding Customer Information, 16 CFR Part 314, Code of Federal Regulations, Title 16, Chapter I, Part 314.
- Sarbanes-Oxley Act of 2002, 15 U.S.C. § 7201, United States Code, Title 15, Chapter 98, § 7201.
- Telecommunications Act of 1996.
- Title III of the Omnibus Crime Control and Safe Streets Act of 1968.
- USA PATRIOT Act of 2001.

2. State statutes and regulations involving:

- Background, preemployment, or other noncriminal justice record checks.
- Categories of case dispositions with special interpretations or purging requirements (for example, diversion, adjournment in lieu of disposition, convictions converted to dismissals if a program is successfully completed).
- Children.
- Children in custody or visitation cases.
- Commercial disclosure of PII, especially unintentionally or stolen.
- Communication intercepts (telephone, e-mail, etc.).
- Confidentiality of information about individuals involved in specific programs or research projects.
- Credit reporting.
- Criminal intelligence system law.
- Criminal justice information system law.
- Denial of licensing or benefits.
- Domestic violence—spousal or partner abuse and elder abuse. This includes the Address Confidentiality Program and its requirements.
- Drivers—Department of Motor Vehicles (DMV) information.
- Education.
- Employee/personnel information.
- Expungement, sealing of arrests, dispositions, and convictions.
- False reports to law enforcement.
- Financial information.
- Gang-related laws.
- Gun control laws—checking before purchase.
- Harassment, civil protective orders, stay-away orders.
- Identity theft.
- Jurors—prospective jurors, trial jurors, or grand jurors.
- Juvenile delinquency.
- Juvenile dependency.
- Law enforcement civilian review boards.
- Mandatory reporting laws—doctors, teachers, counselors, etc.
- Medical—diagnosis and treatment.
- Mental health—evaluations, diagnosis, and treatment.
- PIA requirements.
- Privacy laws. (Refer to Section 8.6, Resources, for the Robert Ellis Smith compilation, *Compilation of State and Federal Privacy Laws*.)
- Problem-solving court provisions.
- Public housing.
- Racial and ethnic profiling.
- Rape shield law.
- Rehabilitation of individuals with convictions, including restoration of civil rights.
- SEARCH, The National Consortium for Justice Information and Statistics, *Compendium of State Laws: Compendium of State Privacy and Security Legislation: Overview 2002*, Criminal History Record Information (i.e., criminal history repository law). Refer to Section 8.6, Resources, for cited references.
- Sex offender registries.

- Substance abuse—diagnosis, evaluations, and treatment.
- Victims of crime; crime victims’ bill of rights.
- Voters.
- Witnesses.

3. Local and tribal laws, resolutions, and ordinances involving:

- Code of Federal Regulations (CFR) that apply to Indian country.
- Contracts regulations and provisions (for example, P.L. 93-638).
- Criminal history repositories.
- Criminal intelligence systems.
- Criminal justice information systems.
- Federal statutes applicable to Indian country.
- Law enforcement review boards.
- Open-meeting laws.
- PIA requirements.
- Public records or freedom of information law.
- State statutes and regulations.
- Tribal codes.
- Tribes may have code provisions or may be subject to federal statutes or regulations that address all of the topics listed above in Category 2.

8.4 Identifying Critical Issues and Policy Gaps

As the legal research is completed, the project team will understand the policy choices that have already been made for the jurisdiction and the entities responsible for making those policy choices. For example, the legal research should identify the jurisdiction’s law or policies that are enacting requirements mandated and those that are not mandated by federal law. The legal research should identify those gaps in the jurisdiction’s law or policies that still need to be addressed. Once the team understands the policy choices and determines whether an existing policy choice should be revisited, it will know whether to address its findings to the state legislature (if the decision is embodied in state statute) or to the specific administrative entity. When current laws and regulations do not address an issue, the team should deliberate based upon the issue’s similarity to other resolved issues.

8.4.1 Identifying Team Members’ Privacy Concerns

While the legal analysis and FIPs will provide a framework and identify issues for the development of the privacy policy, the project team should also determine the team members’ views of privacy issues. The team members will likely deal with information-access issues on a regular basis. They should be aware of the privacy issues that have caused them concern or caused concern for members of the public with whom they interact. The team’s discussions of identified concerns should provide some clarification for policy issues that need to be addressed and help to identify the vision and scope of the policy. Team members represent their own views and those of their constituencies. Active articulation of their perspectives is essential in crafting a solid privacy policy.

8.4.2 Using Legal Research as a Guide

In drafting the privacy policy, it is important to remember to review and articulate prior legal and policy work. The local jurisdiction probably has already enacted a significant amount of privacy laws that reflect the jurisdiction’s policy choices. In developing the privacy policy, it is important to build from existing laws and policies by compiling them into one comprehensive document and restating them in a brief and clear statement of policy.

8.5 Legal Citations Within the Privacy Policy

The results of the legal analysis should be a list of specific legal citations that should be included either in the body of the privacy policy or as an appendix to the policy and cross-referenced throughout the policy provisions where appropriate. It is important to include these citations in the privacy policy for the following purposes:

- To assure those within the entity, those who participate and share or access information with the entity, and the public that the agency is in compliance with legal authority.
- To support and solidify entity privacy provisions and procedures. For example, the privacy policy may identify the different categories of information that are exempt from disclosure (refer to Appendix C.1, SLT Policy Development Template, Section J, Sharing and Dissemination, item 9). Legal citations will be included in the privacy policy to defend the entity's position for certain policy provisions.
- In support of information system transparency (refer to Appendix C.1, SLT Policy Development Template, N. Accountability and Enforcement, N.1. Information System Transparency). Since the privacy policy will be made available to the public, anyone reading the policy should quickly be able to ascertain not only how the entity handles and protects PII but also the legal authority under which the entity has shaped its policies.

8.6 Resources

- Code of Federal Regulations (CFR), Title 28 (28 CFR)—Judicial Administration, Chapter 1—U.S. Department of Justice:
 - Part 20—*Criminal Justice Information Systems*, www.it.ojp.gov/documents/28CFR_Part_20.PDF.
 - Part 22—*Confidentiality of Identifiable Research and Statistical Information*, www.it.ojp.gov/documents/28CFR_Part_22.PDF.
 - Part 23—*Criminal Intelligence Systems Operating Policies*, www.it.ojp.gov/documents/28CFR_Part_23.PDF.
 - Part 46—*Protection of Human Subjects*, www.it.ojp.gov/documents/28CFR_Part_46.PDF.
- Computer Matching and Privacy Protection Act of 1988, Public Law 100-503; 5 U.S.C. § 552a. Records Maintained on Individuals, www.law.cornell.edu/uscode/html/uscode05/usc_sec_05_00000552---a000-.html.
- Driver's Privacy Protection Act of 1994, Public Law 103-322; 18 U.S.C. § 2721. Prohibition on Release and Use of Certain Personal Information From State Motor Vehicle Records, www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002721----000-.html.
- Electronic Communications Privacy Act of 1986, Public Law 99-508; 18 U.S.C. Chapter 121—Stored Wire and Electronic Communications and Transactional Records Access, www.law.cornell.edu/uscode/html/uscode18/usc_sup_01_18_10_I_20_121.html.
- Electronic Privacy Information Center (EPIC), listing of privacy laws by state, www.epic.org/privacy/consumer/states.html.
- Fair Credit Reporting Act of 1970, Public Law 91-508; 15 U.S.C. § 1681. Congressional Findings and Statement of Purpose, www.law.cornell.edu/uscode/html/uscode15/usc_sec_15_00001681----000-.html.
- Freedom of Information Act (FOIA) of 1974, Public Law 104-231; 5 U.S.C. § 552. Public Information; Entity Rules, Opinions, Orders, Records, and Proceedings, Amended fall 1996, www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm.
- Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191, <http://aspe.hhs.gov/admsimp/pl104191.htm>.
- National Association of State Chief Information Officers (NASCIO), Federal Privacy Law Compendium, Version 1.0, April 2003, www.nascio.org/publications/documents/NASCIO-PrivacyLawCompendium.pdf.

- NASCIO, *Information Privacy: A Spotlight on Key Issues*, Compendium of Federal Laws, Version 1.0, February 2004, www.nascio.org/publications/documents/NASCIO-InformationPrivacy2004.pdf.
- National Conference of State Legislatures (NCSL), listing of Privacy Protections in State Constitutions, www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/PrivacyProtectionsinStateConstitutions/tabid/13467/Default.aspx.
- National Criminal Justice Association (NCJA), *Justice Information Privacy Guideline: Developing, Drafting and Assessing Privacy Policy for Justice Information Systems*, Chapter 3, September 2002, www.ncja.org/Content/NavigationMenu/PoliciesPractices/JusticeInformationPrivacyGuideline/default.htm.
- Office of Management and Budget, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, Public Law 107-347, December 17, 2002, www.whitehouse.gov/omb/memoranda/m03-22.html.
- Organisation for Economic Co-operation and Development (OECD), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Fair Information Principles (FIPs), October 26, 2004, http://it.ojp.gov/documents/OECD_FIPs.pdf.
- Privacy Act of 1974, Public Law 93-579; 5 U.S.C. § 552a. Records Maintained on Individuals, www.law.cornell.edu/uscode/html/uscode05/usc_sec_05_00000552---a000-.html.
- Privacy Protection Act of 1980, Public Law 96-440; 42 U.S.C. § 2000aa. Searches and Seizures by Government Officers and Employees in Connection With Investigation or Prosecution of Criminal Offenses, www.law.cornell.edu/uscode/html/uscode42/usc_sec_42_00002000--aa000-.html.
- Right to Financial Privacy Act of 1978, Public Law 95-630; 12 U.S.C. Chapter 35—Right to Financial Privacy, www.law.cornell.edu/uscode/html/uscode12/usc_sup_01_12_10_35.html.
- Safeguarding Against and Responding to the Breach of Personally Identifiable Information, Office of Management and Budget (OMB) Memorandum M-07-16 (May 2007), www.whitehouse.gov/OMB/memoranda/fy2007/m07-16.pdf.
- SEARCH, The National Consortium for Justice Information and Statistics, Compendium of State Laws: *Compendium of State Privacy and Security Legislation: Overview 2002*, Criminal History Record Information, Bureau of Justice Statistics (BJS), revised June 17, 2004, NCJ 200030, bjs.ojp.usdoj.gov/content/pub/pdf/cspsl02.pdf.
- Smith, Robert Ellis. *Compilation of State and Federal Privacy Laws*, ISBN 0-930072-11-1, 2003.
- Telecommunications Act of 1996, S. 652, Federal Communications Commission (FCC), www.fcc.gov/Reports/tcom1996.pdf.
- Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Public Law 90-351; 18 U.S.C. Chapter 119—Wire and Electronic Communications Interception and Interception of Oral Communications, www.law.cornell.edu/uscode/html/uscode18/usc_sup_01_18_10_I_20_119.html.
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act of 2001), H.R. 3162, www.epic.org/privacy/terrorism/hr3162.pdf.
- University of Miami, Florida, Ethics Program, Privacy/Data Protection Project, Selected Federal Privacy Statutes, http://privacy.med.miami.edu/web_laws_regs.htm.
- University of Miami, Florida, Ethics Program, Privacy/Data Protection Project, U.S. Federal Privacy Laws, http://privacy.med.miami.edu/glossary/xd_us_privacy_law.htm.
- U.S. Department of Justice, Bureau of Justice Statistics, Criminal Justice System Flowchart, <http://bjs.ojp.usdoj.gov/content/justsys.cfm>.
- U.S. Department of Justice, Privacy Office, *Privacy Impact Assessments*, www.usdoj.gov/pcl/pia.htm.

Section 9—Writing the Privacy Policy

9.1 Vision and Scope for the Policy

In preparation for drafting the privacy policy, it is assumed that the project team has identified potential issues (through the completion of a Privacy Impact Assessment—refer to Section 4.7), information exchanges have been identified to which the privacy policy will apply (refer to Section 7), and the legal analysis has been completed (refer to Section 8). As a result, applicable law and policies have been identified. Now the team is ready to draft the privacy policy. Defining the vision and scope of the policy is an essential beginning point for the development of the elements of the privacy policy. The team must determine to whom the policy applies, outline the scope of its authority, and define what the policy will cover. A recommended policy outline is provided in Section 9.2, Policy Outline, illustrating the policy topics and concepts that should be covered. These are described in more detail in Section 9.4, Core Policy Concepts. Further, a policy template with sample language is available in Appendix C.1, SLT Policy Development Template.



It is important to note that there will be more than one audience for the privacy policy. This will include not only practitioners who will use the policy to make day-to-day decisions on how to handle a particular piece of information but also members of the public and, potentially, privacy advocate community representatives.

It is acknowledged that although many entities will be addressing similar policy issues, each will likely have unique issues that are relevant to their particular agency. Begin by identifying what the privacy policy will accomplish. For example, the user of this guide could be from a single entity that wishes to develop its own policy or from a participant in a multientity information sharing system. While many of the principles remain the same, there may be particular needs of the local or tribal entity or jurisdiction that do not need to be dealt with by any other entity. For example, tribal groups often have to deal with the overlapping or shared criminal jurisdictions among tribal, state, and federal entities. As a result, tribal policies may have unique features that are not applicable to other groups.

The team should draft a policy that is clear in its vision and scope and is readable and understandable by all audiences, in order to ensure its use and to instill confidence and public trust.

9.2 Policy Outline

The first step in the drafting process is to develop a policy outline. Such an outline should provide guidance on additional research and decision making. A recommended policy outline is shown below and discussed in more detail in Section 9.4.

- Purpose Statement
- Policy Applicability and Legal Compliance
- Governance and Oversight
- Definitions
- Information (what information the entity handles)
- Acquiring and Receiving Information
- Information Quality Assurance
- Collation and Analysis (if applicable)
- Merging Records
- Sharing and Dissemination
- Redress
 - Disclosure
 - Corrections
 - Appeals
 - Complaints
- Security Safeguards
- Information Retention and Destruction
- Accountability and Enforcement
 - Information System Transparency
 - Accountability
 - Enforcement
- Training

While there is no single outline that works best for everyone, there are some elements that should be included in every privacy policy outline. A purpose statement should discuss the importance of privacy in the integrated justice environment and explain what the policy is trying to accomplish. The policy should also include a statement that defines the policy's applicability and should address the collection, access, use, disclosure, expungement, disposition, retention, and quality of justice information. The document should provide the specific legal requirements and policy decisions concerning the handling of particular types of justice information. Section 8, Performing the Legal Analysis, identifies federal laws that apply to information sharing and outlines a process for analyzing local, tribal, and federal laws and regulations. An accountability section should clarify who has the responsibility for implementing and monitoring compliance and should include a discussion of possible sanctions for violation of the policy. Finally, the policy should include an explanation of the process for reviewing and amending the policy on a regular basis.

9.3 Writing the Policy

Once the outline has been drafted, the necessary policy decisions have been identified and discussed, and recommendations have been made regarding the resolution of privacy issues, the project team can begin writing the policy. As mentioned earlier, the policy author(s) should keep in mind the audiences for which it is drafting. Since persons of varying backgrounds, including justice practitioners and members of the general public, may read the policy, it is important for it to be written succinctly and be understandable. In addition, the rationale for the policy choices should be clearly documented. For example, use commentary and, when appropriate, legal citations to support the formal policy language. Including the rationale will provide additional authority for the policy and will provide some guidance for analogous new issues that arise after the policy is adopted.

Even though the project team has already done most of its work in discussing and making recommendations regarding particular policy issues, its work is not complete. The team needs to be involved in the final drafting process. The choice of the language to use in the final document must clearly articulate the intent of the policy. Team members will be a valuable resource in ensuring that the language accurately conveys the message intended.

9.3.1 Making the Policy Choices—Filling in the Gaps

In drafting the actual policy, it is important to consider the following: The local jurisdiction probably has already enacted a significant amount of privacy laws that, while scattered throughout the statutes, nevertheless reflect the jurisdiction's policy choices. In developing the policy, it is important to build from existing laws and policies, compile them into one comprehensive policy, and restate or reference them in a brief and clear statement of policy. When gaps in existing laws are identified or when integration reveals new issues that are not addressed in existing laws, the team should explore those issues and recommend a policy decision that will enhance the goals and purposes of the existing policy choices.

9.4 Core Policy Concepts

This section is provided to assist writers of the policy to understand each of the core policy concepts that should be addressed in the written provisions of a privacy policy, as recommended in Section 9.2, Policy Outline, and contained in the policy template described in Section 9.5.1 and located in Appendix C.1. of this guide. Each core concept is identified by its section reference within the SLT Policy Development Template.

Section A. Purpose Statement

This section illustrates the importance of privacy in the integrated justice environment by explaining what the policy intends to accomplish—"What is the purpose of the privacy policy itself?" The purpose statement will embody both societal values and expectations for the agency itself.

The following is an example of a policy purpose statement:

"The purpose of this privacy policy is to promote agency conduct that complies with applicable federal, state, local, and tribal laws, regulations, and policies and assists all parties in:

- *Ensuring individual privacy, civil rights, civil liberties, and other protected interests.*
- *Maintaining appropriate levels of operational transparency while increasing public safety and national security.*
- *Protecting the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information.*
- *Encouraging individuals or community groups to trust and cooperate with the justice system.*
- *Promoting governmental legitimacy and accountability.*
- *Making the most effective use of public resources allocated to public safety agencies."*

Section B. Policy Applicability and Legal Compliance

This section articulates, clearly, who the policy is applicable to and what laws, statutes, and regulations apply to their conduct.

- Who Is Subject to the Policy?

It is important to identify in the policy who must comply with the policy, such as, agency personnel, authorized users, contractors, participating agencies and, under certain circumstances, information sharing recipients.

- **When Is the Policy Applicable?**

A privacy policy is relevant for all stages of the flow of information (refer to Appendix B, Criminal Justice System Flowchart, for an illustration), including the collection, receipt, maintenance, use, disclosure, and destruction.

- **Legal Compliance**

There are three distinct aspects of legal compliance that a privacy policy should address. The policy should:

1. Articulate the primary legal authority for the agency's collection, receipt, maintenance, use, disclosure, and destruction of information (refer to Section 8, Performing the Legal Analysis).
2. Identify the legal prescriptions protecting privacy.
3. Ensure the compliance of the agency's practices and internal operating policies with the authorities cited above.

Section C. Governance and Oversight

Governance embraces a number of tasks that generally fall into several roles of continuing responsibility: oversight of the agency, updates to the policy, implementation, and enforcement. The policy should identify the individual roles or positions within the entity who are charged with these tasks and the parameters of their responsibilities. The policy should also express the importance of continuing community involvement.

Section D. Definitions

In this section, the team should identify key words or phrases that are regularly used in the policy and for which the team wants to specify a particular meaning. This may include terms that are not commonly known or have multiple meanings or are terms of art (context-specific meaning). Examples might include:

- Personally identifiable information.
- Access.
- Accurate information.
- Criminal history record information.
- Conviction or disposition information.

For examples of recommended definitions, refer to Appendix C.2, Glossary of Terms and Definitions.

Section E. Information

When drafting the policy, it is important to include provisions that state:

- What information may be sought, retained, shared, or disclosed by the entity. This should include the types or categories of information to which the policy applies because there may be different policy provisions for different types of information. For example, criminal intelligence information may have different provisions than those of criminal history information, investigatory information, or suspicious activity reports.
- Whether the entity categorizes information based upon its nature and purpose, usability, and quality.
- Whether limitations are assigned to each type of information reflecting credentialed, role-based levels of access to the information and the information's sensitivity of disclosure.
- Whether the entity requires certain basic descriptive information (metadata) to be entered and associated with each record that will be accessed, used, and disclosed.
- What information may not be sought, retained, shared, or disclosed by the entity; for example, 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. This is an essential core privacy policy provision.

Section F. Acquiring and Receiving Information

The policy should state the policies and procedures for acquiring and receiving information as they address privacy protections. The provisions should specify:

- The applicable state and federal constitution provisions and statutes that govern the techniques and methods the entity may employ when seeking or receiving information.
- Particular considerations regarding information-gathering and investigative techniques, such as a restriction to the least invasive means.
- The extent to which they apply to recipients of information as well as the suppliers.
- The mechanism by which the agency will ensure compliance with applicable laws by external entities that access or share information with the entity.

Section G. Information Quality Assurance

As discussed in Section 4.3.2, Privacy and Information Quality, the quality of information is relevant to the concept of privacy; as such, agencies should address IQ within their privacy policy. IQ provisions should specify:

- The agency's protocols and procedures for ensuring the quality of the information it collects, maintains, and disseminates.
- Whether agency information carries indicators of its quality that are evident to the user (for example, accurate, complete, current, verifiable, and reliable labels) and that are updated as appropriate.
- The agency's mechanisms for periodic review for ensuring continuing quality and for investigating and handling errors and deficiencies, including those discovered through internal processes and through external sources.
- The agency's notification procedures for informing recipients and also originating sources of errors and corrections.

Section H. Collation and Analysis

To the extent that collation and analysis generate new information for the agency's use, which may also be shared or disseminated, it is important that the results of collation and analysis adhere to applicable laws protecting privacy, as well as standards for IQ. To that end, the policy should specify:

- That analysis is conducted by authorized individuals and is within the scope of the permissible agency activities.
- What information is analyzed.
- The agency's underlying purpose for performing analyses.

Section I. Merging Records

One of the common challenges to IQ in the criminal justice context is the phenomenon of duplicate records and the need to ensure that records are merged only when they relate to the same person. When records cannot be matched for the purposes of merging because insufficient criteria are met, an agency may have a procedure for linking or associating together records that may relate to the same individual. The policy provisions should specify:

- That merging is conducted by authorized individuals and that standards and procedures for mergers have been established by the agency.
- The matching criteria the agency uses to merge multiple records allegedly about the same individual, including a description of the number or type of criteria that must be met before a match is made.
- The procedure and criteria for associating records if the matching criteria are not met.

Section J. Sharing and Dissemination

Addressing information sharing within the agency is equally as important as addressing information sharing outside of the agency. The policy should clarify conditions for whether information should be shared and, if so, the conditions and procedures for access and disclosure. The policy provisions on sharing and disclosure should specify:

- Whether records are presumptively accessible (as where a statute declares that records generated by public agencies are open to the public), depending on the various laws and regulations applicable to the agency. If they are presumptively accessible, the policy must describe clearly the limitations on access and cite specific legal authority for each stated basis of denial. If they are presumptively not public (for example, a statute providing juvenile court records are closed), the policy must describe clearly the conditions under which information may or may not be disclosed.
- Whether the levels of access and permissions the agency assigns to each authorized user correlate highly with their identified roles.
- The conditions and credentials by which access to and disclosure of agency records are provided to those within the agency; those in other governmental agencies; those responsible for public protection, public safety, or public health; and those persons authorized by law for specific purposes.
- The policy in place that ensures third-party dissemination is made only in accordance with permissions of the originating agency.
- The acceptable practice relative to the confirming or denial of the existence or nonexistence of a record.

Section K. Redress

Redress can be defined as “to set right, remedy, or rectify.” Although, historically, the right to petition for a redress of a grievance referred only to Congress and the courts, later the due process clause in the Fourteenth Amendment (incorporation doctrine) expanded that right to include all state and federal courts and legislature, plus the executive branches of the state and federal governments. The right to petition also includes the right to sue the government and the right of individuals, groups and, possibly, corporations to lobby the government. Redress addresses public agency responsibilities with regard to disclosure and correction of information and the handling of complaints.

Redress relative to an individual about whom information has been gathered is a policy concept that covers procedures for disclosure, corrections, appeals, and complaints.

Section L. Security Safeguards

As discussed in Section 4.4.2, Privacy and Security, PII needs to be protected with reasonable safeguards against risk of loss or unauthorized access, modification, use, destruction, or disclosure. Provisions should specify the range of administrative, technical, and physical business practices and mechanisms that aim to preserve privacy and confidentiality and the restrictions on information access to authorized users for authorized purposes. The policy should state:

- Who is responsible for the establishment and enforcement of security procedures.
- How the center will protect the information from unauthorized access, modification, theft, or sabotage resulting from natural or human-caused disasters or intrusions.
- That information will be stored in a secure format and a secure environment.
- The credentials of agency personnel whose position and job duties require access.
- Whether audit trails of request and disseminated information are kept and that the log identifies the user initiating the query.
- The procedures for data breach notification.

Section M. Information Retention and Destruction

Every entity should have an established policy on how long to retain different types of information in order to ensure effective records management and compliance with applicable laws and regulations, to ensure that the information is reviewed on a scheduled basis for validation, and to institute methods for purging or destruction. The policy should clearly specify the entity's:

- Review schedule.
- Retention and destruction policies.
- Methods to remove or destroy information.
- Procedure if approval is needed prior to removal or destruction.
- Policy on whether the source of the information is notified prior to removal or destruction.
- Process for keeping records of dates when information is to be removed if not validated prior to the end of its period and whether there is an autogenerated system prompt that a record is due for review.

Section N. Accountability and Enforcement

This policy concept comprises three areas: information system transparency, accountability, and enforcement. An agency should be transparent with regard to its information collection practices, including making the agency privacy policy available to the public, to ensure the public trust by promoting accountability and information for citizens about what justice entities are doing. Accountability can be defined as the obligation of persons or entities to bear consequences or be answerable for the responsibilities conferred on them. Accountability may be dictated or implied by law, regulation, or agreement. Enforcement prescribes the agency's procedures for evaluating compliance and for the authority to enact sanctions or consequences for noncompliance.

The provisions that fall within these policy concepts should specify:

- Whether the agency will be open with the public in regard to information (and intelligence) collection practices.
- Whether the privacy policy is available to the public.
- The point of contact for handling inquiries or complaints.
- Whether electronic access (including the identity of the user initiating the query) is maintained in an audit log.
- The procedures and practices the agency follows to enable evaluation of user compliance,
- The agency's mechanism for personnel to report errors and violations.
- The frequency of audits (annually and randomly) and who conducts them.
- How often the agency reviews and updates the provisions of the privacy policy.
- Procedures for enforcement if a user is found to be in noncompliance with the provisions of this policy.
- The agency's rights with regard to restricting qualifications and number of personnel having access and ability to suspend or withhold service and access to participating agencies or participating agency personnel who violate the privacy policy.

Section O. Training

Training is essential to effective implementation of any policy. The agency should determine who should be required to participate in training (all agency personnel, personnel providing information technology services to the agency, staff in other public agencies or private contractors providing services to the agency, or users who are not employed by the agency) and state this requirement in the privacy policy. Additionally, the policy should briefly describe what is covered by the training program (for example, the purpose of the policy, substance and intent of the provisions of the policy, impact of infractions, and possible penalties for violations). Training individuals who are to be held accountable for the provisions of the privacy policy is a critical agency responsibility to ensure protections are in place. For more information on training, refer to Section 10.4, Training Recommendations.

9.5 Templates to Assist With Drafting the Privacy Policy

The following resource is provided to assist the project team with drafting the privacy policy.

9.5.1 *Privacy, Civil Rights, and Civil Liberties Policy Development Template for State, Local, and Tribal Justice Entities (SLT Policy Development Template)*

This template, contained in Appendix C.1, 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)³⁰ 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 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, IQ, collation and analysis, merging records, information access and disclosure, redress, security safeguards, retention and destruction, accountability and enforcement, and training. For synopses of primary federal laws an agency should review for including in the privacy policy, refer to Appendix C.3 Federal Laws Relevant to Seeking, Retaining, and Disseminating Justice Information.

9.6 Perform a Policy Evaluation

Once a draft policy is developed, SLT agency practitioners should evaluate whether the policy adequately addresses current privacy standards and protection recommendations before the policy is finalized and adopted.

9.6.1 *Policy Review Checklist*

GPIQWG assists the practitioner by providing a mechanism for policy evaluation, the *Privacy, Civil Rights, and Civil Liberties Policy Development Template for State, Local, and Tribal Justice Entities: Policy Review Checklist (or Policy Review Checklist)*, contained in Appendix D. The checklist is a companion piece to the SLT Policy Development Template and serves both as a self-assessment tool to assist privacy policy authors, project teams, and agency administrators in evaluating whether the provisions contained within their draft policy have met the core concepts recommended in the template, as well as a useful resource for the annual policy review. The checklist is structured according to policy categories and section references that correlate checklist components with those in the template.

9.7 Vetting the Privacy Policy

A concise executive summary of three pages or less is a valuable tool for vetting, for review by citizens and executives, and for use at the time of publication (refer to Section 10.2, Publication).

The draft privacy policy should be broadly disseminated for comment before it is finalized. During the team's deliberations, the project team leader should encourage the team members to consult with their constituencies and keep them apprised of the progress of the privacy policy development. The team members should also be encouraged to share the draft policy with their constituents. While significant input should come from the team members who represent large groups, such as police chiefs or sheriffs, additional input should be sought, before the policy is finalized, from others who were not involved on the team. With this input, additional persons will have been given an opportunity to comment or express concerns about the policy.

How and when others are consulted should be agreed upon by the project team. During the drafting process, it may be appropriate to bring specific issues that need to be resolved to the attention of constituencies for their input. As an initial draft is prepared, it may be appropriate to allow small groups or selected individuals to review portions of the draft. However, the team must be careful not to circulate drafts too early or circulate too many versions of the draft in order to avoid confusion or distribution of incomplete information.

³⁰ 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) entities; federal entities; and the private sector to facilitate terrorism-related information sharing, access, and collaboration.

9.8 Process for Revisions and Amendments

Provisions should be included in the policy for the regular and systematic review of the privacy policy to keep it current and relevant. The privacy policy should be reviewed in light of new laws (statutory or regulatory), court decisions, changes in technology, changes in the purpose and use of the information systems, and changes in public expectations.

9.9 Resources

- American Bar Association (ABA), American Jury Project, *Principles for Juries and Jury Trials, Principle 7— Courts Should Protect Juror Privacy Insofar as Consistent With the Requirements of Justice and the Public Interest*, 2005, www.abanet.org/juryprojectstandards/principles.pdf.
- National Center for State Courts (NCSC), Public Access to Court Records, www.ncsc.org/Topics/Access-and-Fairness/Privacy-Public-Access-to-Court-Records/Resource-Guide.aspx.

State policies are constantly evolving. This is one resource for the latest developments in state-level policies and practices related to court records and associated issues.

- Steketee, M. W., and A. Carlson, *Developing CCJ/COSCA Guidelines for Public Access to Court Records: A National Project to Assist State Courts*. Williamsburg, VA: National Center for State Courts. Final report to the State Justice Institute (SJI-01-N-054 and SJI-02-N-007), October 18, 2002, <http://www.it.ojp.gov/docdownloader.aspx?ddid=1534> and revised report, October 15, 2005, <http://www.it.ojp.gov/docdownloader.aspx?ddid=1535>.

Section 10—Implementing the Privacy Policy

10.1 Formal Adoption of the Policy

At some point, an appropriate governing body should formally adopt the entity's privacy policy. The first step for adoption should be approval by the project team itself. If the project team is working under the auspices of some other governing board, approval should be sought from the governing board as well. The governing body may have existing protocols for considering and adopting policies that may require that the draft be published for comment for a certain period of time or require public hearings before the governing body. As discussed earlier, the privacy policy may not necessarily contain any new concepts. For the most part, it will include a compilation of laws and rules that regulate information sharing in the justice system synthesized to address the particular concerns of privacy. The privacy policy puts existing laws and regulations into context and may recommend areas requiring policy attention (laws, policies, practices). Depending on the nature of those parts of the policy, the project team may need to seek approval from the legislature.



10.2 Publication

The adopted privacy policy should be readily available to justice decision makers,³¹ practitioners, and the general public. The policy should be available to all executives of entities involved in the development and implementation of processes; to local, tribal, and state elected or appointed officials; and the media. The electronic version should be available in a format suitable for downloading from Web sites, internal and public, of all entities participating in the justice information sharing system. The policy should also be incorporated into training curriculum for entity staff and users.

10.3 Outreach

If the team has done a thorough job of involving stakeholders and conducting a transparent development and implementation process, outreach to the larger community should be relatively easy. Since all individuals and entities, including potential opponents, were involved in the process, these representatives can act as emissaries to their colleagues and constituencies. The people who have been involved in developing the policy will have an established rapport and credibility with their peers and can relate the rationale behind the policy.

³¹ Global Justice Information Sharing Initiative (Global) Privacy and Information Quality Working Group (GPIQWG), *Executive Summary for Justice Decision Makers: Privacy, Civil Rights, and Civil Liberties Program Development*, Appendix A.1, within this guide.

Even with an extensive network of involved individuals, the project team leader, as a representative of the project champion or sponsor, should conduct more formal outreach. This type of outreach can include:

- Press releases and briefings.
- Briefings for elected or appointed local, state, and tribal officials, especially members of the governing body, whether it is a county commission or the state legislature.
- Community hearings.
- Establishment of a volunteer speakers' bureau to provide presentations on request to civic organizations or other groups.

For Indian tribes and communities, outreach and community education are essential because tribal assumptions about privacy are different from state or federal assumptions. Outreach should begin with presentations to the tribal governing body (i.e., tribal councils and judges) and justice system staffs. Outreach should include articles in tribal newspapers to inform tribal citizens.

The purpose of the outreach strategy is to inform the public about the thoughtful, intentional process used to develop the policy and to promote public confidence in the justice entity and in the safety and integrity of the PII contained in justice systems.

10.3.1 *Guidance for Building Communities of Trust*³²

Guidance for Building Communities of Trust (BCOT), developed by Robert Wasserman in collaboration with the Office of Community Oriented Policing Services (COPS), U.S. Department of Justice, and the U.S. Department of Homeland Security, focuses on developing relationships of trust among law enforcement, fusion centers, and the communities they serve, particularly immigrant and minority communities, so that the challenges of crime control and prevention of terrorism can be addressed. Lessons learned have been documented from a series of roundtable discussions held across the country among state and major urban area fusion centers, local law enforcement, and community advocates. The resulting guidance provides advice and recommendations on how to initiate and sustain trusting relationships that support meaningful sharing of information, responsiveness to community concerns and priorities, and the reporting of suspicious activities. The importance for communities and law enforcement to build and maintain trusting relationships to prevent acts of crime and terrorism is the overarching theme of this document.

10.4 Training Recommendations

Training is essential to effective implementation of any privacy policy. Each team should determine and recommend an approach to training based on the particular organizational structures, existing training programs, and available resources. At a minimum, a subgroup of the team should be assigned to begin development of training recommendations at the inception of the project team.

Before completion of the privacy policy, the initial training recommendations may provide outlines rather than substantive content for training to allow for specific process needs. The legal analysis will be completed before the formal policy is written so that work on training materials for understanding the legal environment can begin.

Taking into consideration the size of the justice entity, available resources, existing training programs, and the nature of the training to be undertaken, the following areas should be addressed in the team's training recommendations.

10.4.1 Trainees

Determine what personnel should be required to participate in training regarding the implementation of and adherence to the privacy policy. At a minimum, consider trainees from the following groups: senior management, information technology staff, new employees, current employees who perform processes

³² Robert Wasserman, *Guidance for Building Communities of Trust*, Office of Community Oriented Policing Services, U.S. Department of Justice, and the U.S. Department of Homeland Security, www.cops.usdoj.gov/files/RIC/Publications/e071021293_BuildingCommTrust.pdf.

that are impacted by this policy, and those individuals who use the information in their day-to-day jobs. Others to consider include participating agency personnel, personnel providing information technology services to the entity, staffing in other public entities or private contractors providing services to the entity, etc.

10.4.2 Content

Determine what should be covered by the training program. Training, at minimum, should address two broad areas:

1. The purpose of the policy, the substance of the policy and its importance to the entity's mission and responsibility, impact of infractions, and possible penalties for violations.
2. How to implement the policy in the day-to-day work of the user, whether a paper or systems user. Additional topics may include:
 - 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 entity responsibilities and obligations under applicable law and policy.
 - The impact of improper activities associated with infractions within or through the entity.
 - 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.

10.4.3 Method

Different approaches to training include lecture courses, distance learning, computer-based training, train-the-trainer courses, line officer briefings, and course modules added to existing training programs. Refer to Section 10.4.5.1, Privacy Training Resources, for a listing of established privacy training resources recommended to assist the entity in this effort.

10.4.4 Frequency

There is no question that along with the initial training plan, there should be periodic training updates, refresher materials, and training provided. The critical element is that the project team recommendation contemplates periodic retraining and updates for all users who are affected by the privacy policy.

10.4.5 Additional Resources and Training Tools

Consider whether additional resources might assist users as they begin to implement the privacy policy. For example, should the project team develop a checklist of steps to follow for certain job functions that could be at the desktop? Would a Web site with frequently asked questions (FAQs) or a Help Desk be helpful?

Also consider incorporating existing privacy, civil rights, and civil liberties-focused publications and resources into the entity's training efforts.

10.4.5.1 Privacy Training Resources

The following are primers and training resources that may be useful when introducing privacy policy concepts for training sessions.

- ***Executive Summary for Justice Decision Makers: Privacy, Civil Rights, and Civil Liberties Program Development***

This executive summary is an awareness resource for justice executives, as well as an informational tool to use for training. The easy-to-read flyer is designed to engender awareness about the topic, make the case for privacy policy development, and underscore the importance of promoting privacy protections within justice agencies. Included is information on basic privacy concepts; the intersection between privacy,

security, and information quality; privacy risks; and steps to establish privacy protections through a privacy program cycle. This paper applies settled privacy principles to justice information sharing systems and makes recommendations on best practices. Refer to Appendix A.1, within this guide, to view this executive summary or download it online at www.it.ojp.gov/privacy.

- ***7 Steps to a Privacy, Civil Rights, and Civil Liberties Policy***

Designed for both justice executives and agency personnel, this document raises awareness and educates readers on the seven basic steps involved in the preparation for development of a privacy, civil rights, and civil liberties policy (as recommended in this **Privacy Guide**). Each step describes the practical tasks associated with preparing for, drafting, and implementing a privacy policy. Also featured is an overview of the core concepts (or chapters) that an agency should address in the written provisions of a privacy policy (as recommended in the Template). Refer to Appendix A.2, within this guide, to view this document or download it online at www.it.ojp.gov/privacy.

- ***The Importance of Privacy, Civil Rights, and Civil Liberties Protections in American Law Enforcement and Public Safety***

A training video, titled *The Importance of Privacy, Civil Rights, and Civil Liberties Protections in American Law Enforcement and Public Safety*, was developed by Global's Intelligence Working Group (GIWG) Privacy and Training Committees. This eight-minute video is a training tool designed to educate viewers, particularly line officers during roll call, on the privacy and civil liberties issues they may confront in their everyday work and the liabilities associated with the failure to adhere to sound policy and practice.

Though officers receive privacy training as part of their academy training, it is important to regularly reinforce the importance of upholding these protections. This short overview will review and proactively emphasize the role line officers have in the ongoing protection of citizens' and community members' privacy, civil rights, civil liberties, and other associated rights in the course of officers' daily activities and calls for service. This video can be viewed online at www.ncirc.gov/privacylineofficer/.

- ***Suspicious Activity Reporting Line Officer Training CD***

This SAR CD was developed through a joint effort of BJA, DOJ, and the International Association of Chiefs of Police (IACP) to educate law enforcement line officers not only on what kinds of suspicious behaviors are associated with pre-incident terrorism activities and how to document and report suspicious activity but also on how to ensure the protection of privacy, civil rights, and civil liberties when documenting SAR information. The CD also provides information about the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) requirement that NSI sites have privacy policies in place prior to NSI participation. This CD can be viewed online at <http://nsi.ncirc.gov/SARLOT/>.

- ***Criminal Intelligence Systems Operating Policies (28 CFR Part 23) Online Training***

Criminal intelligence plays a vital role in the safety and security of our country. The Code of Federal Regulations, Title 28, Part 23 – Criminal Intelligence Systems Operating Policies (or 28 CFR Part 23) was issued in 1980 to ensure the privacy and constitutional rights of individuals during the collection and exchange of criminal intelligence information, and it has since been an important part of the intelligence landscape.

28 CFR Part 23 is a guideline for law enforcement agencies that operate federally funded multijurisdictional criminal intelligence systems. To facilitate greater understanding of 28 CFR Part 23, the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, developed the Criminal Intelligence Systems Operating Policies (28 CFR Part 23) online training, which focuses on the requirements of 28 CFR Part 23 and includes topics such as compliance, privacy, inquiry, and dissemination requirements; storage requirements; and review-and-purge requirements.

The online training is available at www.ncirc.gov or www.iir.com/Justice_Training/28cfr/default.aspx.

- ***Criminal Intelligence Sharing: Protecting Privacy, Civil Rights, and Civil Liberties***

This training is designed to present effective information sharing tools, examine the principles of 28 CFR Part 23, and address the importance of privacy, civil rights, and civil liberties in the context of information sharing. Its purpose is to enhance information sharing by clarifying the various rules and regulations to ensure that agencies are more confident as they collect and share information, particularly criminal intelligence information. In addition, technical assistance can be provided through on-site system reviews, policy reviews, and other specialized problem resolution. Training and technical assistance for this project are provided through funding from BJA, DOJ. For more information on this training, visit www.iir.com/Justice_Training/privacy101/default.aspx.

- **DHS/DOJ Privacy and Civil Liberties Web Portal**

Through a joint effort among DHS, DOJ, and BJA, this collaborative Web portal, accessible at www.it.ojp.gov/PrivacyLiberty, provides access to a wide range of resources and training materials available in the Information Sharing Environment that address privacy and civil liberties protections, including many of the Global products described in this guide. Although originally intended for fusion center use, these resources can easily be adapted by law enforcement, criminal justice, public safety, and homeland security communities nationwide.

10.4.6 Acknowledgment

For accountability purposes, there should be some active acknowledgment that the privacy policy and training on the policy were received within the entity, such as a signed statement of policy receipt, review, and agreement to comply with the policy.

10.4.7 How Will You Measure Your Success?

When developing the training plan, include performance measurement as the final piece of the plan. Consider that the measurement of training success may be rolled into the overall method of measuring the success of the policy. As long as the project team considers what the training is supposed to accomplish, articulates such, and follows a chosen approach to ensure that it has succeeded, the team's training goal will be met.

10.5 Privacy Officer

The tasks of continued implementation, monitoring, and compliance should be the responsibility of a trained Privacy Officer—whether a full-time Privacy Officer position or the occupant of a different position who is assuming these responsibilities. Ideally, someone experienced in privacy, civil rights, and civil liberties issues should be appointed and trained, such as through the Privacy Training Resources cited in Section 10.4.5.1, to be the agency's Privacy Officer prior to (or during) the development of the privacy policy and will serve on the policy development team. This individual may or may not be the same person designated as the project champion or project team leader. Once the policy has been drafted, this individual will maintain primary oversight and managerial responsibility for ensuring continued policy implementation, training, monitoring, and compliance. Traditional Privacy Officer responsibilities include:

- Routine review of the entity's information privacy procedures to ensure that they are comprehensive and up to date.
- When additional or revised procedures may be called for, work with relevant entity offices in the consideration, adoption, and implementation of such procedures.
- Review existing departmental and component-level privacy policies and procedures to ensure the entity's full compliance with local, state, and federal laws, regulations, and policies relating to information privacy.

- Oversee the implementation of privacy protections in personnel procedures and information system processes.
- If applicable to the entity's function, review and approve all analytical products for appropriate privacy, civil rights, and civil liberties protections prior to dissemination or sharing by the entity.
- Handle reported errors and violations of the provisions of the privacy policy.
- Ensure that enforcement procedures and sanctions (which should be outlined in the privacy policy) are adequate and enforced.
- Receive and respond to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s) maintained or accessed by the entity.
- Manage the evaluation of user compliance (for example, through the use of system audits).
- Serve as a point of contact for handling individuals' requests for corrections involving information the entity has disclosed and can change because it originated the information. The Privacy Officer will inform individuals of the procedure for requesting and considering requested corrections, including appeal rights.

10.6 Monitoring Policy Implementation

A scheme or plan for evaluation and continued monitoring of the implementation of the policy should be in place before the policy is implemented. It is far easier to gain a commitment to ongoing evaluation and monitoring when the investment of the team is high, at the inception of the project, than as an afterthought after the policy is fully developed and on the verge of implementation.

The evaluation should ask such questions as:

- Does the privacy policy, as implemented, respond to the purposes and goals defined in the beginning?
- Is the policy responsive to the legal demands identified at the outset?
- Does the policy have to be updated in response to events occurring since the inception of the project?
- Is any of the justice data that is shared inaccurate, and what can be done to minimize that occurrence?

10.6.1 *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise*

For justice agencies with an intelligence function, the *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise* document assists intelligence enterprises in complying with all applicable privacy, civil rights, and civil liberties protection laws, regulations, and policies. As a next step for agencies that have completed and implemented a privacy policy, the checklist evaluates agency compliance with the policies and procedures the agency has established in their privacy policy and helps to uncover any gaps that may need to be addressed in policies, technology, or procedures. The checklist provides a suggested methodology for conducting the review of an agency's intelligence enterprise and identifies the high-liability areas of concern that should be included when performing the review.

10.7 Ensuring Compliance

As part of policy implementation, ensuring that personnel and authorized users are complying with the policies established in the privacy policy is important. The entity needs to 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 the policy and applicable law. This will include logging access to these systems and periodic auditing, so as to not establish a pattern of the audits. Audit logs of queries made to the system should identify the user initiating the query, and an audit trail of accessed, requested, or disseminated information should be maintained.

10.8 Enforcement

It is important to identify who is responsible for enforcement of the privacy policy. Traditionally, this is a role of the Privacy Officer. The entity should establish and clearly document the entity's procedures for addressing violations of the provisions of the privacy policy regarding the collection, use, retention, destruction, sharing, classification, or disclosure of PII. An entity may:

- Suspend or discontinue access to information by the user.
- Suspend, demote, transfer, or terminate the person, as permitted by applicable personnel policies.
- Apply administrative actions or sanctions as provided by entity rules and regulations or as provided in entity personnel policies.
- If the user is from an external entity, request that the relevant entity, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions.
- Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.
- Restrict the qualifications and number of personnel having access to entity information and suspend or withhold service and deny access to any participating entity or participating entity personnel violating the entity's privacy policy.

10.9 Resources

- American Society for Training & Development (ASTD), formed in 1944, www.astd.org/ASTD/aboutus/about_inside.htm.

ASTD is the world's largest association dedicated to workplace learning and performance professionals.

- *Criminal Intelligence Systems Operating Policies (28 CFR Part 23) Online Training*, Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, www.ncirc.gov or www.iir.com/Justice_Training/28cfr/default.aspx.
- *Criminal Intelligence Sharing: Protecting Privacy, Civil Rights, and Civil Liberties*, Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, www.iir.com/Justice_Training/privacy101/default.aspx.
- DHS/DOJ Privacy and Civil Liberties Web Portal, U.S. Department of Homeland Security and U.S. Department of Justice, www.it.ojp.gov/PrivacyLiberty.
- Global's *Implementing Privacy Policy in Justice Information Sharing: A Technical Framework*, www.it.ojp.gov/privacy.
- Global's *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise*, www.ncirc.gov/documents/public/supplementaries/privacy_verification.pdf.
- Global's *Suspicious Activity Reporting Line Officer Training CD*, <http://nsi.ncirc.gov/SARLOT/>.
- Global's *The Importance of Privacy, Civil Rights, and Civil Liberties Protections in American Law Enforcement and Public Safety* video, www.ncirc.gov/privacylineofficer/.
- McNamara, Carter, Authenticity Consulting, LLC, *Employee Training and Development: Reasons and Benefits*, Free Management Library, The Management Assistance Program for Nonprofits, 1999, www.managementhelp.org/trng_dev/basics/reasons.htm.
- *Training* magazine, www.trainingmag.com.

Training magazine is a 41-year-old professional development magazine that advocates training and workforce development as a business tool. The magazine delves into management issues, such as leadership and

succession planning; human resources (HR) issues, such as recruitment and retention; and training issues, such as learning theory, on-the-job skills assessments, and alignment of core workforce competencies to enhance the bottom-line impact of training and development programs. Written for training, human resources, and business management professionals in all industries, *Training* combines a primarily paid circulation with a small percentage of qualified, controlled recipients to deliver the strongest circulation in the market.

- The following GPIQWG privacy primers are contained within the appendices of this guide and are also available online at www.it.ojp.gov/privacy.
 - *Executive Summary for Justice Decision Makers: Privacy, Civil Rights, and Civil Liberties Program Development*, Appendix A.1 of this guide.
 - *7 Steps to a Privacy, Civil Rights, and Civil Liberties Policy*, Appendix A.2 of this guide.

Appendix A—Privacy Primers

Using the following two executive primers, entity administrators are made aware of the importance of having privacy policies within their entity and are provided with a high-level overview of the steps an entity should follow to develop a privacy policy.

These primers may also be downloaded online at www.it.ojp.gov/privacy. To request printed copies, send requests to GLOBAL@iir.com.

A.1 Executive Summary for Justice Decision Makers: Privacy, Civil Rights, and Civil Liberties Program Development

This executive summary is an awareness resource for justice executives, as well as an informational tool to use for training. The easy-to-read flyer is designed to engender awareness about the topic, make the case for privacy policy development, and underscore the importance of promoting privacy protections within justice agencies. Included is information on basic privacy concepts; the intersection between privacy, security, and information quality; privacy risks; and steps to establish privacy protections through a privacy program cycle. This paper applies settled privacy principles to justice information sharing systems and makes recommendations on best practices.

A.2 7 Steps to a Privacy, Civil Rights, and Civil Liberties Policy

Designed for both justice executives and agency personnel, this document raises awareness and educates readers on the seven basic steps involved in the preparation for development of a privacy, civil rights, and civil liberties policy (as recommended in this Privacy Guide). Each step describes the practical tasks associated with preparing for, drafting, and implementing a privacy policy. Also featured is an overview of the core concepts (or chapters) that an agency should address in the written provisions of a privacy policy (as recommended in the SLT Development Template).



United States Department of Justice

Executive Summary for Justice Decision Makers: Privacy, Civil Rights, and Civil Liberties Program Development

Decision makers within the justice and public safety communities must vigorously protect information privacy, civil rights, and civil liberties. Establishing and implementing these protections will guide an agency's information gathering and collection, storage, and sharing efforts and strengthen trust and public confidence by promoting effective and responsible sharing of information that supports fundamental privacy concepts. Difficult? Yes. Insurmountable? No.

What Is Privacy?

Privacy is a core right protected by federal and state constitutions and expected by citizens. Protecting information privacy, a subset of broader privacy interests, is a fundamental responsibility of justice agencies that collect and share personally identifiable information. Privacy is not just the right to be left alone or the right to be free from unreasonable searches and seizures or the freedom of association. Rather, privacy also includes the fair gathering, collection, and use of personally identifiable information. Privacy policies articulate appropriate gathering and collection of and allowable uses for information and provide accountability for misuse.

What Are Civil Rights and Civil Liberties?¹

The term "civil liberties"² generally means the freedom from intrusive or undue government interference, while "civil rights"³ refers to the rights of individuals to participate fairly and equally in society and the political process. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference.

Privacy, civil rights, and civil liberties interests—or "privacy" interests—embrace all privacy interests, whether rooted in civil rights law, civil liberties guarantees, or the protection of information privacy interests of individuals or organizations.

What Are the Risks of Not Having Privacy Protections?

Given today's enhanced ability to gather, collect, store, and share vast amounts of personally identifiable information, a well-developed privacy, civil rights, and civil liberties protection policy can help an agency prevent problems. Failure to develop, implement, and maintain appropriate protections for both information and use of technology can result in:

- Harm to individuals.
- Public criticism and loss of confidence in and cooperation with the agency.
- Lawsuits and liability.
- Limited ability to share information.
- Proliferation of agency databases with inaccurate or incomplete data.
- Damage to the credibility of agencies that act on inaccurate or incomplete data.

Privacy Scenarios and Their Relation to Privacy Protection Policies

The following are privacy scenarios that can occur in any jurisdiction across the country. Each may have a number of privacy-related consequences, though only one or more are illustrated.



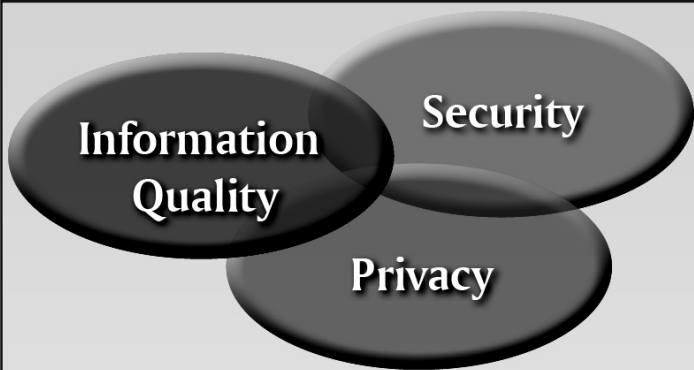
Office of Probation and Parole Sued by Domestic Violence Victim

A domestic violence victim won a lawsuit filed against the department of corrections' probation and parole office and received \$250,000 in damages after being revictimized by her ex-spouse, a probation officer who accessed her information in a database containing her new address. The couple had recently divorced because of reports of repeated domestic violence, and the woman had moved to a different part of the state. Despite the allegations, the department had not limited the officer's system access or permissions, nor had the woman's electronic record been assigned proper security to ensure that the location of her new residence was withheld from unauthorized access. The probation officer was fired and is awaiting criminal proceedings.

Consequence: Harm to individuals and financial costs for the agency.

www.it.ojp.gov/privacy

(continued on page 3)



How Does Privacy Intersect With Information Quality and Security?

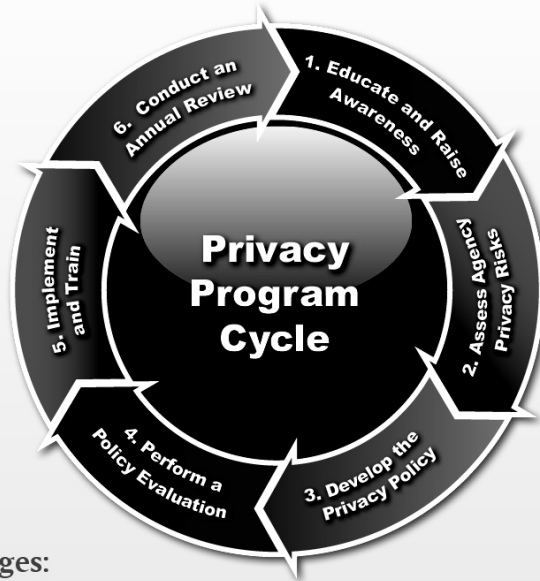
Information quality plays an extremely important role in the protection of privacy rights of individuals. Issues of privacy and information quality (IQ) are inherently linked, because both influence the appropriate use of justice information. Entity privacy policies should address information quality issues. In practice, the accuracy, timeliness, completeness, and security of information connected to an individual or organization may raise as many concerns as the release of the information or its public availability.

Security relates to how an organization protects information during and after collection. Privacy addresses why and how information is collected, handled, and disclosed and is concerned with providing reasonable quality control regarding that information. Security policies implement privacy policies by ensuring compliance with the manner and extent to which information is allowed to be shared by the privacy policies. Having a security policy related to data or information is not enough. Security policies alone do not adequately address the privacy, civil rights, civil liberties, and IQ issues contemplated in this discussion. Considering the breadth of the issue, some existing privacy policies may fail to address these concerns in that they relate to access to records instead of defining privacy protections both in procedures and in system processes.



What Can You Do to Establish Privacy Protections?

Privacy is not a project; privacy is an ongoing program. As entities consider establishing and implementing privacy protections for the information they collect, store, maintain, access, and share through their business processes and procedures, they are encouraged to follow the stages recommended in the Privacy Program Cycle.



Stages:

- 1. Educate and Raise Awareness** on the importance of having privacy, civil rights, and civil liberties protections within the agency.
- 2. Assess Agency Privacy Risks** by evaluating the process through which your agency collects, stores, protects, shares, and manages information.
- 3. Develop the Privacy Policy⁴** to articulate the legal framework and policy position of an organization on how it handles information the agency seeks or receives and uses in the normal course of business.
- 4. Perform a Policy Evaluation** to determine whether the privacy policy adequately addresses current standards and privacy protection recommendations.
- 5. Implement and Train** personnel and authorized users on the established rules and procedures.
- 6. Conduct an Annual Review** and make appropriate changes in response to implementation experience, applicable law, technology, and public expectations.

www.it.ojp.gov/privacy

Why Develop Privacy Policies?

A comprehensive privacy program serves as a fundamental lynchpin to developing a system of trust that allows agencies to share personally identifiable and other sensitive information. There needs to be trust—not only within and between justice partners sharing information but also by the public, whose information is being collected and utilized—that justice agencies are serving as responsible stewards of their personally identifiable information and operating with respect for individual privacy and the law. Without this trust, information sharing initiatives will not thrive and are ultimately doomed to public condemnation and civil liability.

Where to Turn for More Information

To support justice agencies in their efforts to implement privacy, civil rights, and civil liberties policies and protections for the information they collect, store, maintain, access, and share, the U.S. Department of Justice's (DOJ) Global Justice Information Sharing Initiative (Global) has published a *Global Privacy Resources* booklet as a road map to guide justice entities through the diverse resources available for each stage of the Privacy Program Cycle. The resources presented are developed for state, local, and tribal (SLT) entities by DOJ's Global or Global partners or through DOJ collaborations with other federal agencies, such as the U.S. Department of Homeland Security (DHS). To view this *Global Privacy Resources* booklet, as well as all resources for a Privacy Program Cycle, refer to www.it.ojp.gov/privacy. To request printed copies, send requests to GLOBAL@iir.com.

Privacy Scenarios and Their Relation to Privacy Protection Policies (continued from page 1)

Report Details Missteps in Data Collection



Intimate information was collected about the lives of 52,000 people and stored in an intelligence database accessible to about 12,000 federal, state, and local law enforcement authorities and to certain foreign governments. This organization did so without systematically retaining evidence that its data collection was legal, without ensuring that the data it obtained met its needs or requests, without discovering or reporting abuses, without providing clear policy guidance, and without following retention regulations. Lawmakers called the violations unacceptable and permanently shut the database down. **Consequence: Loss of ability to gather information.**

Judge Limits Police Taping



In rebuke of a surveillance practice greatly expanded by a police department after the September 11 attacks, a federal judge ruled that police must stop the routine videotaping of people at public gatherings unless there is an indication that unlawful activity may occur. In the ruling, the judge found that the police department had not followed established guidelines under which police are allowed to conduct investigations, including videotaping of political events only if there are indications that unlawful activity may occur and only after obtaining the proper permissions, neither of which had occurred. **Consequence: Loss of public confidence in law enforcement and loss of support.**

Officer Leaks Suspicious Activity Report Details



While socializing with a friend after work, a police officer talked about a suspicious activity report he had read in which the friend's neighbor was suspected of a possible sex crime involving young teens. That privacy breach quickly turned into a rumor that spread throughout the community. The person said to be a suspect, as well as his family members, immediately became victims of harassment and the brunt of jokes around town. Less than a week later, the investigation revealed that the neighbor was not the perpetrator but, in fact, it was someone who had traveled to the community from a neighboring state. Even though the rumor proved false, the casual leaking of information caused permanent damage to the reputation of the individual and his standing in the community. **Consequence: Demonstrable harm to an individual's reputation and loss of public trust in the agency.**

www.it.ojp.gov/privacy

About Global

www.it.ojp.gov/global

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

DOJ's Global Advisory Committee (GAC) recommends that local, state, tribal, and federal justice decision makers make privacy protections a priority. 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.



This project was supported by Grant No. 2009-DB-BX-K105 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.

About the Global Privacy and Information Quality Working Group (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 executive summary to support justice agencies in their efforts to educate agencies and raise awareness of the importance of establishing and implementing a privacy program.

Footnotes

1 For more information on privacy, civil rights, and civil liberties, refer to the U.S. Department of Justice (DOJ) Global Justice Information Sharing Initiative's (Global's) *Privacy, Civil Rights, and Civil Liberties Policy Development Guide for State, Local, and Tribal Justice Entities*, Section 4: Understanding Foundational Concepts.

2 According to DOJ's Global, 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.

3 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.

4 The authors acknowledge that agencies may already have privacy policies in place (for example, in Standard Operating Procedures) that may need to be reviewed and updated as part of this step in the Privacy Program Cycle.

rev. 9/6/11



7 Steps to a Privacy, Civil Rights, and Civil Liberties Policy



United States
Department of Justice

Ethical and legal obligations compel professionals in the justice system, when sharing information, to protect privacy, civil rights, and civil liberties interests. The U.S. Department of Justice's Global Justice Information Sharing Initiative's (Global) *Privacy, Civil Rights, and Civil Liberties Policy Development Guide for State, Local, and Tribal Justice Entities* (or "Privacy Guide") is a practical resource that supports privacy protection requirements for physical and automated information sharing environments. Its purpose is to guide privacy policy development while supporting information sharing.



The following seven steps highlight the privacy policy development process, as recommended in the Privacy Guide, including preparation, drafting, and implementation. Privacy Guide section references are also included along with each step. The Privacy Guide is available at www.it.ojp.gov/privacy.

Step 1. Understanding Foundational Concepts (Section 4)

- Become familiar with applicable terms: privacy, civil rights, civil liberties, information quality, and security
- Learn how privacy issues arise and the purpose of a privacy policy

Step 2. Assembling the Project Team (Section 5)

- Designate the project champion or sponsor
- Secure support and justify resources
- Appoint the project team leader
- Build the project team and stakeholders
- Identify the roles within the entity (e.g., privacy and security officers)

Step 3. Establishing a Charter (Section 6)

- Draft components:
 - Vision, mission, and values statements
 - Goals and objectives for the creation of the privacy policy
- Write the charter

Step 4. Understanding Information Exchanges (Section 7)

- Identify information exchanges—what information is collected, used, maintained, and shared
- Examine privacy risks by performing a Privacy Impact Assessment

Step 5. Performing the Legal Analysis (Section 8)

- Identify legal authorities applicable to the entity's privacy protection efforts
- Address legal and technological gaps in the privacy policy

Step 6. Writing the Privacy Policy (Section 9 and Appendix C)

- Develop an outline and draft policy language to meet core privacy policy concepts. Include legal references identified in Step 5
- Perform a policy review to determine whether the draft policy adequately addresses current privacy standards and protection recommendations

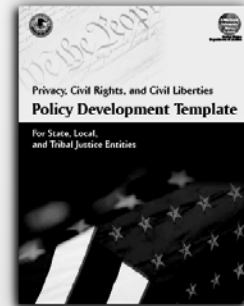
Step 7. Implementing the Privacy Policy (Section 10)

- Obtain formal adoption of the policy
- Make the policy available to decision makers, practitioners, and the public
- Train personnel and authorized users
- Specify methods for auditing and compliance monitoring
- Incorporate revisions and updates identified through the monitoring process

www.it.ojp.gov/privacy

Core Concepts Recommended in a Privacy Policy

The following core concepts should be addressed in a privacy policy, as recommended by the *Privacy, Civil Rights, and Civil Liberties Policy Development Template for State, Local, and Tribal Justice Entities* (or “SLT Policy Development Template”). These are discussed further in Section 9 of the Privacy Guide and in the Template located in Appendix C. Template sections are referenced along with each concept. The SLT Policy Development Template is available at www.it.ojp.gov/privacy.



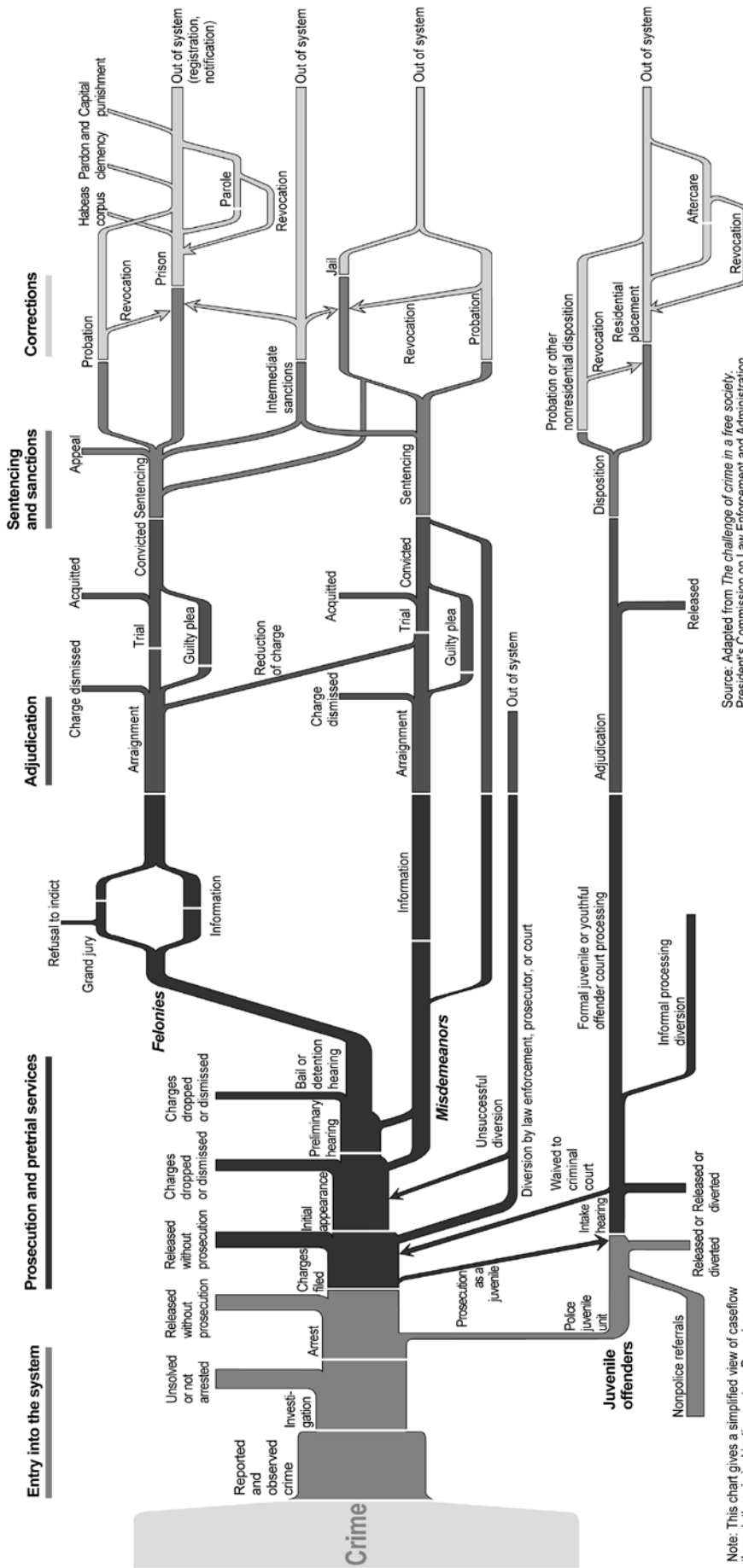
- Section A. Purpose Statement**—What is the purpose of the privacy policy? Articulate the importance of privacy in the agency’s integrated justice environment, and explain what the policy will accomplish.
- Section B. Policy Applicability and Legal Compliance**—To whom does the policy apply and under what authority does the entity operate? Articulate what laws, statutes, and regulations apply to the entity’s conduct and to its operating policies.
- Section C. Governance and Oversight**—Who is responsible for oversight, development, implementation, and enforcement of the policy? Identify those charged with these tasks and their responsibilities.
- Section D. Definitions**—What key words or phrases are regularly used in the policy? Define terms that are not commonly known or have multiple meanings.
- Section E. Information**—What information does the policy apply to and how is it handled? Identify information that may or may not be sought, retained, shared, or disclosed and the processes for labeling and categorizing the information, including limitations of its use.
- Section F. Acquiring and Receiving Information**—What are the policies that require that information be obtained legally? State the agency’s position that information acquired or received must comply with applicable law.
- Section G. Information Quality Assurance**—How is information quality addressed? State the process for ensuring the quality of collected, maintained, and disseminated information.
- Section H. Collation and Analysis**—What are the parameters for collation and analysis? State who is authorized, what information is analyzed, and for what purpose.
- Section I. Merging Records**—What are the parameters for merging records? State who is authorized, the criteria for merging, and the policy for partial matches.
- Section J. Sharing and Dissemination**—What are the conditions for sharing information inside and outside the agency? Identify levels of access, credentials, policies, and the public records process.
- Section K. Redress**—What is the process for disclosure and correction of information? State the conditions for disclosure to individuals and the procedures for corrections, appeals, and complaints.
- Section L. Security Safeguards**—How is information kept secure? Specify the administrative, technical, and physical mechanisms to secure information and breach notification procedures.
- Section M. Information Retention and Destruction**—How long is information retained? State the retention period and procedures for the review, purge, and destruction of information.
- Section N. Accountability and Enforcement**—How do you ensure transparency, accountability, and enforcement? Specify how the policy is provided to the public, the schedule for policy updates, the point of contact for inquiries and complaints, the process for reporting violations and evaluating compliance, and sanctions for noncompliance.
- Section O. Training**—What are the training requirements for the privacy policy? State who is required to receive privacy policy training and what is covered by the training.

Appendix B—Criminal Justice System Flowchart

Criminal Justice System Flowchart Bureau of Justice Statistics, U.S. Department of Justice

This chart and a discussion of the events in the criminal justice system are available online at <http://bjs.ojp.usdoj.gov/content/justsys.cfm>.

What is the sequence of events in the criminal justice system?



Note: This chart gives a simplified view of caseload through the criminal justice system. Procedures vary among jurisdictions. The weights of the lines are not intended to show actual size of caseloads.

Source: Adapted from *The challenge of crime in a free society*, President's Commission on Law Enforcement and Administration of Justice, 1967. This revision, a result of the Symposium on the 30th Anniversary of the President's Commission, was prepared by the Bureau of Justice Statistics in 1997.



Appendix C— Privacy Policy Drafting Tools

Use the following tools when drafting the justice entity's privacy policy:

C.1 *Privacy, Civil Rights, and Civil Liberties Policy Development Template for State, Local, and Tribal Justice Entities* (SLT Policy Development Template)

The SLT Policy Development Template may also be downloaded online at www.it.ojp.gov/privacy. To request printed copies, send requests to GLOBAL@iir.com.

C.2 *Glossary of Terms and Definitions*

C.3 *Federal Laws Relevant to Seeking, Retaining, and Disseminating Justice Information*

C.1 *Privacy, Civil Rights, and Civil Liberties Policy Development Template for State, Local, and Tribal Justice Entities*

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 C.2, Glossary of Terms and Definitions, within the *Privacy, Civil Rights, and Civil Liberties Policy Development Guide for State, Local, and Tribal Justice Entities*] 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 C.2, Glossary of Terms and Definitions, within the *Privacy, Civil Rights, and Civil Liberties Policy Development Guide for State, Local, and Tribal Justice Entities* [Privacy Guide])]).

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 C.2, Glossary of Terms and Definitions, within the Privacy Guide)] 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 C.3 Federal Laws Relevant to Seeking, Retaining, and Disseminating Justice Information of the Privacy Guide.)

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, of this template)] 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 C.2, Glossary of Terms and Definitions, within the Privacy Guide.

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 C.2, Glossary of Terms and Definitions, within the Privacy Guide.) 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 C.2, Glossary of Terms and Definitions, within the Privacy Guide 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 C.3 of the Privacy Guide 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?**

Best Practice: 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:

- Is exempt from disclosure,
- Has been or may be shared through the ISE,
 - Is held by the [name of entity] and
 - 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?**

Note: 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.

Best Practice: 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 of this template).]

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.

C.2 Glossary of Terms and Definitions

The following is a list of primary terms and definitions used throughout this guide and within Appendix C.1, *Privacy, Civil Rights, and Civil Liberties Policy Development Template for State, Local, and Tribal Justice Entities*. 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.³³

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 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.

³³ 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.

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.

C.3 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 C.2 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.



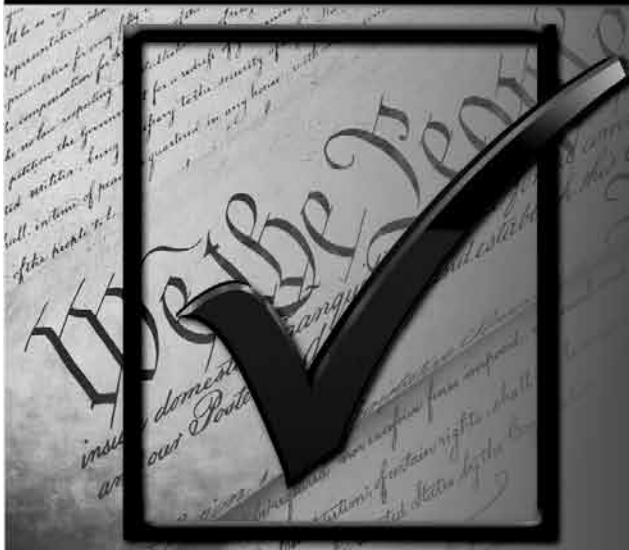
Appendix D—*Policy Review Checklist*

The *Policy Review Checklist* may also be downloaded online at www.it.ojp.gov/privacy. To request printed copies, send requests to GLOBAL@iir.com.



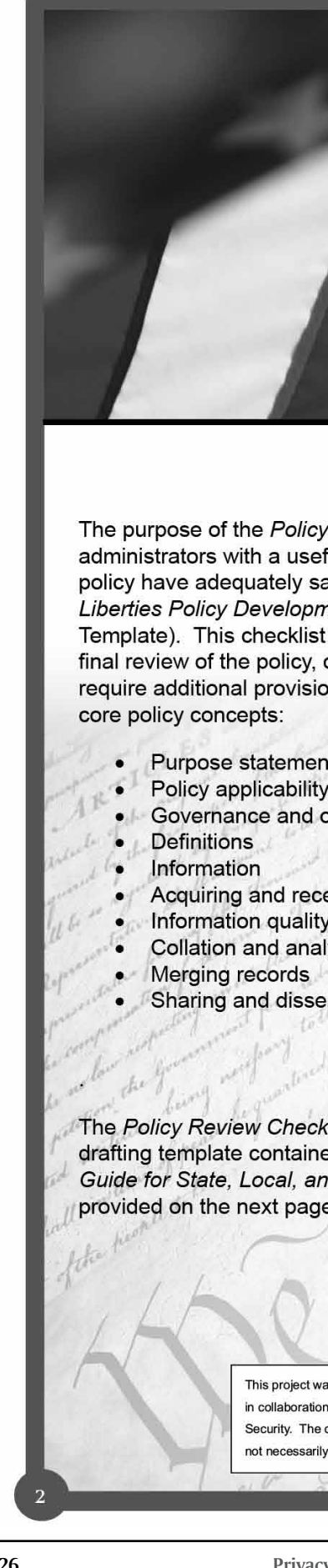
United States
Department of Justice

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



Policy Review Checklist





Privacy, Civil Rights, and Civil Liberties Policy Development Template for State, Local, and Tribal Justice Entities: **POLICY REVIEW CHECKLIST**

INTRODUCTION

The purpose of the *Policy Review Checklist* is to provide privacy policy authors, project teams, and agency administrators with a useful tool for evaluating whether the provisions contained within the entity's privacy policy have adequately satisfied the core concepts recommended in the *Privacy, Civil Rights, and Civil Liberties Policy Development Template for State, Local, and Tribal Justice Entities* (SLT Policy Development Template). This checklist may be used during the drafting process to check work on the draft policy, during the final review of the policy, or during an annual review to determine areas that may need minor enhancement or require additional provisions to ensure that the policy is comprehensive in addressing all of the recommended core policy concepts:

- Purpose statement
- Policy applicability and legal compliance
- Governance and oversight
- Definitions
- Information
- Acquiring and receiving information
- Information quality assurance
- Collation and analysis
- Merging records
- Sharing and dissemination
- Redress
 - Disclosure
 - Corrections
 - Appeals
 - Complaints
- Security safeguards
- Information retention and destruction
- Accountability and enforcement
 - Information system transparency
 - Accountability
 - Enforcement
- Training

The *Policy Review Checklist* is a companion resource to the SLT Policy Development Template—a policy-drafting template contained in the appendix of the *Privacy, Civil Rights, and Civil Liberties Policy Development Guide for State, Local, and Tribal Justice Entities* (Privacy Guide). A description of each of these resources is provided on the next page.

This project was supported by Grant No. 2009-DB-BX-K105 awarded by the Bureau of Justice Assistance, Office of Justice Programs, in collaboration with the U.S. Department of Justice's Global Justice Information Sharing Initiative and the U.S. Department of Homeland Security. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the U.S. Department of Justice or the U.S. Department of Homeland Security.

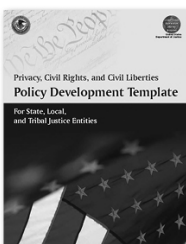
The following resources can be found online at www.it.ojp.gov/privacy. To request printed copies, send requests to GLOBAL@iir.com.

Privacy, Civil Rights, and Civil Liberties Policy Development Guide for State, Local, and Tribal Justice Entities
(Privacy Guide)



The Privacy Guide is a practical, hands-on tool for SLT justice practitioners charged with development and implementation of a privacy policy, providing sensible guidance for articulating privacy obligations in a manner that protects the justice agency, the individual, and the public. This guide provides a well-rounded approach to the planning, development, and implementation of and education on agency privacy protections. Also included are drafting tools, such as a policy template (described next), a glossary, legal citations, and sample policies.

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



Included in the Privacy Guide is the SLT Policy Development Template, which was developed to assist SLT agencies in crafting the language of privacy policy provisions related to the information the entity collects, receives, maintains, archives, accesses, and discloses to entity personnel, governmental agencies, and other participating criminal justice and public safety agencies, as well as to private contractors and the general public. Each section represents a fundamental component of a comprehensive policy that includes baseline provisions on information collection, information quality, collation and analysis, merging, access and disclosure, redress, security, retention and destruction, accountability and enforcement, and training. 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.



HOW TO USE THIS CHECKLIST

The format of this checklist was designed to mirror the structure and provisions recommended in the SLT Policy Development Template. Privacy policy provisions are grouped according to core policy concepts.

With both the agency privacy policy and the checklist in hand, reviewers are guided to read each question in the checklist; compare it with the language in the privacy policy, noting the section and page number in the checklist; and indicate whether the provision has been fully met, has been partially met, was not addressed, or is not applicable. Comments and suggestions can be added where needed.

If the policy author(s) followed the format and flow of the SLT Policy Development Template when drafting the policy, completing this checklist should be a simple process since each checklist question sequentially mirrors the structure of the template. Thus the reviewer will find it a fluid process to move through both documents—the agency privacy policy and the checklist—in tandem as the review is performed. Policy authors are not required, however, to follow the outline and format of the SLT Policy Development Template in order to use this review checklist. The checklist will still readily illuminate for the reviewer whether each recommended provision has been satisfied, requiring only minor additional effort to locate the policy language in the draft policy in order to score it in the checklist.

Annual Review

In addition to its use during the privacy policy drafting process, this checklist is also designed for use in the annual review of the policy. As recommended by the Privacy Guide, justice entities are encouraged to review and update the provisions protecting privacy, civil rights, and civil liberties contained in the privacy policy at least **annually**. Annual updates will ensure that appropriate revisions are made in response to changes in applicable laws, technology, the purpose and use of the information systems, and public expectations. This in turn will ensure that systems and individuals are enabled to comply with the most current protections established in the entity privacy policy.



Checklist Column Headings

To assist reviewers in navigating the policy review checklist, the following information is provided to describe the purpose and use of each of the checklist's column headings.

Template Section—Each question is grouped according to core policy provision concepts and reflects Sections A. through O. of the SLT Policy Development Template. This column indicates the template section in which the question is contained.

Does the entity's privacy policy clearly state the following—Each recommended provision in the SLT Policy Development Template is reworded here as an evaluation question, asking the reviewer whether the entity's privacy policy has addressed the relevant template provision. Questions are numbered in the same sequence as the provisions in the template.

Page/section in policy—For cross-referencing and future review purposes (for example, if there is more than one draft), this column enables the reviewer to indicate where in the policy the provision is located. This is especially useful when a provision, upon review, is found to be partially met; the author can quickly locate the provision in the policy to make the needed revisions.

Criteria met—A checkbox for the reviewer to indicate whether the privacy policy provision has fully satisfied the recommended core concept.

Criteria partially met—A checkbox for the reviewer to indicate that the privacy policy provision only "partially" satisfies the recommended core concept and requires further revision. An explanation should be recorded in the Comments/Suggestions area.

Criteria not addressed—A checkbox for the reviewer to indicate that the criteria were not addressed in the privacy policy, requiring further work. An explanation should be recorded in the Comments/Suggestions area.

Not applicable (N/A)—A column to indicate that the provision is not applicable to the entity or the entity's functions and procedures. If appropriate, an explanation can be recorded in the Comments/Suggestions area.

Comments/Suggestions—An area for documenting guidance, suggested language, and other comments (for example, partially met criteria, criteria that were not addressed, or criteria that are not applicable).

Annual Review: Check if provision requires update—A checkbox to be used by the individual performing the annual review to indicate that the provision requires revisions.

Annual Review: Was the provision revised?—A checkbox to be used by the policy author to communicate to the reviewer(s) that the provision was updated.

Annual Review Comments—An area for documenting justifications for needed revisions (e.g., legislative change), comments, and other recommendations.

Special Provisions

A. Information Sharing Environment

Provisions—Since the provisions in this checklist mirror those contained in the SLT Policy Development Template, provisions that relate to the Information Sharing Environment (ISE)¹ are boxed. If the entity is not participating in ISE-related initiatives, the boxed portion of the policy provisions may be disregarded during the policy review; however, they are left in this document 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).

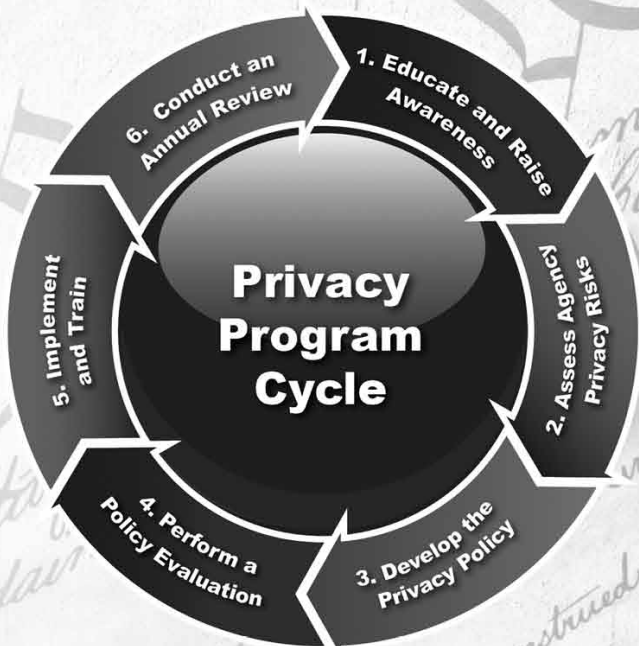
B. Suspicious Activity Report Provisions

As reflected in the SLT Policy Development Template, this checklist includes provisions that are specifically applicable to suspicious activity reporting (SAR) to assist those entities that collect SARs in developing appropriate policies and protections for this type of information. SAR provisions are shaded. If the entity does not collect SAR information, the shaded portion of the policy provisions may be disregarded.

¹ For more information on the Information Sharing Environment, refer to the SLT Policy Development Template, Introduction, Section C.1 The Information Sharing Environment or www.ise.gov.

ADDITIONAL PRIVACY RESOURCES

Once an entity has reviewed its privacy policy using this checklist and has made revisions to ensure that the published version satisfies all applicable core concepts recommended in the SLT Policy Development Template, the next stage is to determine how to implement these established protections in the entity's system and procedures and how to train personnel and authorized users. For information on resources designed to meet these needs, as well as other resources available for all stages of the Privacy Program Cycle, refer to the *Global Privacy Resources* booklet, available at www.it.ojp.gov/privacy. To request printed copies, send requests to GLOBAL@iir.com.



About Global

www.it.ojp.gov/global

The U.S. Department of Justice's Global Justice Information Sharing Initiative (Global) serves as a Federal Advisory Committee to the U.S. Attorney General on critical justice information sharing initiatives. Global promotes standards-based electronic information exchange to provide justice and public safety communities with timely, accurate, complete, and accessible information in a secure and trusted environment. Global is administered by the U.S. Department of Justice (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 checklist to support justice agencies in their efforts to develop comprehensive privacy protections policies. For more information on GPIQWG, refer to: www.it.ojp.gov/gpiqwg. To download a copy of this checklist refer to www.it.ojp.gov/privacy. To request printed copies, send requests to GLOBAL@iir.com.

Agency Name: _____

Person Completing Review: _____

Title: _____

Template Section	Policy Provision Checklist			
	Does the entity's privacy policy clearly state the following:	Page/section in policy	Criteria met	Criteria partially met
A. Purpose Statement	1. 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)?		<input type="checkbox"/>	<input type="checkbox"/>
B. Policy Applicability and Legal Compliance	1. Who is subject to the privacy policy (who must comply with the policy; for example, entity personnel, participating agencies, and private contractors)?		<input type="checkbox"/>	<input type="checkbox"/>
	2. The method(s) by which the policy is made available to personnel, participating users, and individual users (for example, in print, online, etc.)? Whether the entity requires personnel and participating users to acknowledge receipt of the policy and agreement to comply with the policy in writing?		<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>
	3. That personnel and participating information-originating and user agencies must 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? The primary laws with which personnel and participating users must comply?		<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>
	4. Whether the entity's internal operating policies 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? Whether these laws, statutes, and regulations are cited in the privacy policy?		<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>

Policy Review Checklist

Review Date: _____

Phone: _____

E-mail: _____

				Annual Review Checklist		
Criteria not addressed	Not applicable (N/A)	Comments/Suggestions	Check if provision requires update	Was the provision revised?		Annual Review Comments
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No		
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No		
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No		
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No		
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No		
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No		
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No		
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No		

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

Template Section	Policy Provision Checklist			
	Does the entity's privacy policy clearly state the following:	Page/section in policy	Criteria met	Criteria partially met
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 the privacy policy? Which individual will ultimately be held accountable for the operation of the system and for any problems or errors?		<input type="checkbox"/>	<input type="checkbox"/>
	2. Whether the entity has a privacy oversight committee or team that is responsible for the development of the privacy policy and/or that will routinely review and update the policy?		<input type="checkbox"/>	<input type="checkbox"/>
	3. Whether there is a designated and trained privacy officer who will handle reported errors and violations and oversee the implementation of privacy protections and who will ensure that the entity adheres to the provisions of the ISE Privacy Guidelines and other requirements for participation in the ISE?		<input type="checkbox"/>	<input type="checkbox"/>
	Does the policy identify 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?		<input type="checkbox"/>	<input type="checkbox"/>
	The contact information for the privacy officer (for example, phone, Web site, e-mail, or U.S. mail address)?		<input type="checkbox"/>	<input type="checkbox"/>
	4. Who is responsible for ensuring that enforcement procedures and sanctions for noncompliance with the privacy policy are adequate and enforced?		<input type="checkbox"/>	<input type="checkbox"/>
D. Definitions	1. The key words or phrases (and definitions) that are regularly used in the policy for which the entity wants to specify particular meanings?		<input type="checkbox"/>	<input type="checkbox"/>

Policy Review Checklist

			Annual Review Checklist		
Criteria not addressed	Not applicable (N/A)	Comments/Suggestions	Check if provision requires update	Was the provision revised?	Annual Review Comments
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	

Template Section	Policy Provision Checklist			
	Does the entity's privacy policy clearly state the following:	Page/section in policy	Criteria met	Criteria partially met
E. Information	<p>1. What information may be sought, retained, shared, disclosed or disseminated by the entity (e.g., based on a criminal predicate, threat, or reasonable suspicion)?</p> <p>Whether there are different policy provisions for different types of information (e.g., 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)?</p>		<input type="checkbox"/>	<input type="checkbox"/>
	<p>2. What information may not be sought, retained, shared, or disclosed by the entity (e.g., for reasons of discrimination)?</p>		<input type="checkbox"/>	<input type="checkbox"/>
	<p>3. Whether the entity applies labels to the information (or ensures that the originating entity has applied labels) that indicate to the authorized user that the information:</p> <ul style="list-style-type: none"> • 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? To what extent organizations are protected by the policy? • 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 (e.g., there may be laws that restrict who can access information, how information can be used, and limitations on the retention or disclosure of certain types of information, such as the identity of a sexual assault victim)? 		<input type="checkbox"/>	<input type="checkbox"/>
	<p>4. Whether the entity categorizes information (or ensures 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?</p>		<input type="checkbox"/>	<input type="checkbox"/>

Policy Review Checklist

			Annual Review Checklist		
Criteria not addressed	Not applicable (N/A)	Comments/Suggestions	Check if provision requires update	Was the provision revised?	Annual Review Comments
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	

Template Section	Policy Provision Checklist			
	Does the entity’s privacy policy clearly state the following:	Page/section in policy	Criteria met	Criteria partially met
	<p>5. When information is gathered or collected and retained by the entity, whether the entity assigns labels (by record, data set, or system of records) and whether the entity assigns limitations to identify who is allowed to see (access) and use the information (for example, credentialed, role-based levels of access)?</p>		<input type="checkbox"/>	<input type="checkbox"/>
	<p>6. The conditions that prompt the labels cited in E.5 to be reevaluated?</p>		<input type="checkbox"/>	<input type="checkbox"/>
	<p>7. Whether the 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”) and, if so, whether the entity maintains and adheres to policies and procedures for:</p> <ul style="list-style-type: none"> • 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 agencies? • Access and dissemination (data retrieval and dissemination)—The process of making the information available to other agencies and obtaining feedback on investigative outcomes? • Retention and security of the information? <p>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.</p>		<input type="checkbox"/>	<input type="checkbox"/>

Policy Review Checklist

			Annual Review Checklist		
Criteria not addressed	Not applicable (N/A)	Comments/Suggestions	Check if provision requires update	Was the provision revised?	Annual Review Comments
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	

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

Template Section	Policy Provision Checklist			
	Does the entity's privacy policy clearly state the following:	Page/section in policy	Criteria met	Criteria partially met
	<p>8. Whether the 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?</p>		<input type="checkbox"/>	<input type="checkbox"/>
	<p>9. For purposes of sharing terrorism-related information through the ISE, the entity's 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.</p> <p>Whether the entity has 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 through the ISE, such that participants can handle the information in accordance with applicable legal requirements?</p>		<input type="checkbox"/>	<input type="checkbox"/>
	<p>10. Whether the entity requires 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?</p> <ul style="list-style-type: none"> • Basic information may include, where relevant and appropriate, the name of the originating entity or agency, department, component, and subcomponent (where 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, where feasible, the date its accuracy was last verified. • The title and contact information for the person to whom questions regarding the information, including its accuracy, should be directed. 		<input type="checkbox"/>	<input type="checkbox"/>

Policy Review Checklist

			Annual Review Checklist		
Criteria not addressed	Not applicable (N/A)	Comments/Suggestions	Check if provision requires update	Was the provision revised?	Annual Review Comments
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	

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

Template Section	Policy Provision Checklist			
	Does the entity's privacy policy clearly state the following:	Page/section in policy	Criteria met	Criteria partially met
	11. Whether the entity attaches (or ensures 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?		<input type="checkbox"/>	<input type="checkbox"/>
	12. Whether the entity maintains a record of the source of the information sought and collected?		<input type="checkbox"/>	<input type="checkbox"/>
F. Acquiring and Receiving Information	1. Whether there are 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? The specific applicable laws relevant to seeking and receiving information?		<input type="checkbox"/>	<input type="checkbox"/>
	2. Whether the entity's SAR process provides for human review and vetting to ensure that information is both legally gathered and, where applicable, determined to have a potential terrorism nexus? 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?		<input type="checkbox"/>	<input type="checkbox"/>
	3. Whether the entity's SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved in activities that have been determined to be consistent with criminal activities associated with terrorism will be documented and shared through the ISE?		<input type="checkbox"/>	<input type="checkbox"/>
	4. Whether the entity (if operational, conducting investigations) adheres to a policy regarding the investigative techniques the entity will follow when acquiring information (for example, an intrusion-level statement)?		<input type="checkbox"/>	<input type="checkbox"/>
	5. Whether the agencies that access and share information with the entity are also required to adhere to the applicable laws and policies identified in F.1?		<input type="checkbox"/>	<input type="checkbox"/>
	6. Whether the entity contracts with commercial databases and, if so, how the entity ensures that the commercial database company is in legal compliance in its information-gathering techniques?		<input type="checkbox"/>	<input type="checkbox"/>

Policy Review Checklist

			Annual Review Checklist		
Criteria not addressed	Not applicable (N/A)	Comments/Suggestions	Check if provision requires update	Was the provision revised?	Annual Review Comments
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	

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

Template Section	Policy Provision Checklist			
	Does the entity's privacy policy clearly state the following:	Page/section in policy	Criteria met	Criteria partially met
	7. 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?		<input type="checkbox"/>	<input type="checkbox"/>
G. Information Quality Assurance	1. Whether the entity has established procedures and processes (manual and electronic) to ensure the quality (for example, accurate, complete, current, verifiable, and reliable) of the information it collects and maintains?		<input type="checkbox"/>	<input type="checkbox"/>
	2. Whether the entity applies labels (or ensures that the originating agency has applied labels) to the information regarding its level of quality (for example, accurate, complete, current, verifiable, and reliable)?		<input type="checkbox"/>	<input type="checkbox"/>
	3. Whether the entity researches alleged or suspected errors and deficiencies (or refers them to the originating agency)? How the entity responds to confirmed errors or deficiencies?		<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>
	4. Whether the entity reevaluates (or ensures 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?		<input type="checkbox"/>	<input type="checkbox"/>
	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?		<input type="checkbox"/>	<input type="checkbox"/>

Policy Review Checklist

			Annual Review Checklist		
Criteria not addressed	Not applicable (N/A)	Comments/Suggestions	Check if provision requires update	Was the provision revised?	Annual Review Comments
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	

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

Template Section	Policy Provision Checklist			
	Does the entity's privacy policy clearly state the following:	Page/section in policy	Criteria met	Criteria partially met
	<p>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, whether the entity notifies the originating agency or the originating agency's privacy officer?</p> <p>The method used to notify the agency (written, telephone, or electronic notification)?</p>		<input type="checkbox"/>	<input type="checkbox"/>
	<p>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, whether the entity notifies the external agency?</p> <p>The method used to notify the agency (written, telephone, or electronic notification)?</p>		<input type="checkbox"/>	<input type="checkbox"/>
H. Collation and Analysis	<p>1. Who is authorized (position/title, credentials, clearance level[s], etc.) to analyze information acquired or accessed by the entity?</p>		<input type="checkbox"/>	<input type="checkbox"/>
	<p>2. What information is analyzed (refer to Section E., Information)?</p>		<input type="checkbox"/>	<input type="checkbox"/>
	<p>3. For what purpose(s) the information is analyzed? Best practice: Does the entity's privacy officer or privacy oversight committee review [and approve] all analytical products prior to dissemination or sharing by the entity?</p>		<input type="checkbox"/>	<input type="checkbox"/>
I. Merging Records	<p>1. Who is authorized (position/title, credentials, clearance level[s], etc.) to merge records?</p>		<input type="checkbox"/>	<input type="checkbox"/>

Policy Review Checklist

			Annual Review Checklist		
Criteria not addressed	Not applicable (N/A)	Comments/Suggestions	Check if provision requires update	Was the provision revised?	Annual Review Comments
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	

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

Template Section	Policy Provision Checklist			
	Does the entity's privacy policy clearly state the following:	Page/section in policy	Criteria met	Criteria partially met
	<p>2. What matching criteria does the 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?</p>		<input type="checkbox"/>	<input type="checkbox"/>
	<p>3. If the criteria specified in I.2 are not met, what is the entity's procedure for associating records?</p> <p>Note: If the entity does not merge or associate records that have partial matches, then the policy should state this.</p>		<input type="checkbox"/>	<input type="checkbox"/>
J. Sharing and Disclosure	<p>1. What types of user actions and permissions are controlled by the entity's access limitations? Best practice: It is suggested that entities specify their method for identifying user actions and permissions in their privacy policies.</p> <p>Note: User actions and permissions are often used to identify agencies and individuals with a "need to know" and "right to know" particular information or intelligence, to access case management information, to access nonpersonally identifiable information (PII) only, or to identify who is authorized to submit or modify particular records or record sets, to have read-only access or to be authorized to add/modify/delete records, or to be authorized to grant privileges.</p>		<input type="checkbox"/>	<input type="checkbox"/>
	<p>2. For suspicious activity report information, whether the entity uses a standard reporting format and commonly accepted data collection codes and whether the entity's SAR information sharing process complies with the ISE Functional Standard for suspicious activity reporting?</p>		<input type="checkbox"/>	<input type="checkbox"/>

Policy Review Checklist

				Annual Review Checklist		
Criteria not addressed	Not applicable (N/A)	Comments/Suggestions	Check if provision requires update	Was the provision revised?	Annual Review Comments	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No		
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No		
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No		
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No		

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

Template Section	Policy Provision Checklist			
	Does the entity's privacy policy clearly state the following:	Page/section in policy	Criteria met	Criteria partially met
	<p>3. 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?</p> <p>Whether an audit trail is 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.</p>		<input type="checkbox"/>	<input type="checkbox"/>
	<p>4. Whether participating agencies that access information from the entity are required to obtain approval from the originator of the information prior to further dissemination or to follow the disclosure laws applicable to the originating entity?</p>		<input type="checkbox"/>	<input type="checkbox"/>
	<p>5. 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?</p> <p>Whether an audit trail is 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.</p>		<input type="checkbox"/>	<input type="checkbox"/>
	<p>6. Under what circumstances access to and disclosure of a record is provided to a member of the public in response to an information request, and whether these circumstances are described in the entity's redress policy?</p> <p>Whether an audit trail is 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.</p> <p>Note: This 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.</p>		<input type="checkbox"/>	<input type="checkbox"/>

Policy Review Checklist

			Annual Review Checklist		
Criteria not addressed	Not applicable (N/A)	Comments/Suggestions	Check if provision requires update	Was the provision revised?	Annual Review Comments
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	

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

Template Section	Policy Provision Checklist			
	Does the entity's privacy policy clearly state the following:	Page/section in policy	Criteria met	Criteria partially met
	<p>7. The conditions under which release of information retained by the entity will be provided for specific purposes in response to requests by persons authorized by law?</p> <p>Whether an audit trail is kept of access to and disclosure of information retained by the entity (e.g., dissemination logs, algorithms) and the specific retention period? Refer to N.2, Accountability, for more information on audit logs.</p>		<input type="checkbox"/>	<input type="checkbox"/>
	8. Under what circumstances and to whom the entity will not disclose records and information?		<input type="checkbox"/>	<input type="checkbox"/>
	<p>9. The categories of records that will ordinarily not be provided to the public pursuant to applicable legal authority?</p> <p>Citations to applicable legal authority for each category listed?</p>		<input type="checkbox"/>	<input type="checkbox"/>
	10. The entity's policy on confirming the existence or nonexistence of information to persons or agencies that are not eligible to receive the information?		<input type="checkbox"/>	<input type="checkbox"/>
<p>K. Redress K.1 Disclosure</p>	<p>Disclosure</p> <p>1. If required by state statute, the conditions under which the entity will disclose information to an individual about whom information has been gathered?</p> <p>Whether a record is kept of all requests and of what information is disclosed to an individual?</p> <p>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 privacy policy in lieu of using the sample language provided.</p>		<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>

Policy Review Checklist

			Annual Review Checklist		
Criteria not addressed	Not applicable (N/A)	Comments/Suggestions	Check if provision requires update	Was the provision revised?	Annual Review Comments
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	

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

Template Section	Policy Provision Checklist			
	Does the entity's privacy policy clearly state the following:	Page/section in policy	Criteria met	Criteria partially met
K.2 Corrections	<p>2. The conditions under which the entity will not disclose information to an individual about whom information has been gathered?</p> <p>Citations to applicable legal authority for each stated basis (condition) for denial?</p> <p>Whether the entity refers the individual to the agency originating the information?</p>		<input type="checkbox"/>	<input type="checkbox"/>
	<p>Corrections</p> <p>1. The entity's procedure for handling individuals' requests for correction involving information the entity has disclosed and can change because it originated the information?</p> <p>Whether the entity maintains a record of requests for corrections?</p>		<input type="checkbox"/>	<input type="checkbox"/>
K.3 Appeals	<p>Appeals</p> <p>1. If requests for disclosure or corrections are denied, what is the entity's procedure for appeal?</p>		<input type="checkbox"/>	<input type="checkbox"/>
K.4 Complaints	<p>Complaints</p> <p>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?</p> <p>Whether the entity's privacy officer or designee or other individual is responsible for handling complaints?</p> <p>Whether contact information (for example, phone, Web site, e-mail, or U.S. mail address) is provided for the individual who handles complaints?</p> <p>Whether the entity maintains a record of complaints and requests for corrections?</p>		<input type="checkbox"/>	<input type="checkbox"/>

Policy Review Checklist

			Annual Review Checklist		
Criteria not addressed	Not applicable (N/A)	Comments/Suggestions	Check if provision requires update	Was the provision revised?	Annual Review Comments
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	

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

Template Section	Policy Provision Checklist			
	Does the entity's privacy policy clearly state the following:	Page/section in policy	Criteria met	Criteria partially met
	<p>2. How the entity determines which complaints involve information that is specifically protected information shared through the ISE?</p> <p>Note: This question needs to be addressed when a entity does not have a procedure applicable to all protected information under Section K.4, 1.</p>		<input type="checkbox"/>	<input type="checkbox"/>
L. Security Safeguards	<p>1. Whether the entity has a designated security officer? Whether training is provided for security officers? If the role is a component of another position, whether the policy identifies the title of the position upholding security officer responsibilities?</p>		<input type="checkbox"/>	<input type="checkbox"/>
	<p>2. The entity's physical, procedural, and technical safeguards for ensuring the security of entity data? (Does the policy 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?)</p>		<input type="checkbox"/>	<input type="checkbox"/>
	<p>3. Whether the entity utilizes a separate repository system for tips, leads, and SAR information?</p>		<input type="checkbox"/>	<input type="checkbox"/>
	<p>4. The requirements that ensure that the information will be stored in a secure format and a secure environment?</p>		<input type="checkbox"/>	<input type="checkbox"/>
	<p>5. The required credentials of entity personnel authorized to have access to entity information?</p>		<input type="checkbox"/>	<input type="checkbox"/>
	<p>6. Whether electronic access to entity data identifies the user?</p>		<input type="checkbox"/>	<input type="checkbox"/>
	<p>7. Whether a log is kept of accessed and disseminated entity data and whether an audit trail is maintained? Refer to N.2, Accountability, for more information on audit logs.</p>		<input type="checkbox"/>	<input type="checkbox"/>
	<p>8. Whether risk and vulnerability assessments (if maintained) are stored separately from publicly available data?</p>		<input type="checkbox"/>	<input type="checkbox"/>
	<p>9. The entity's procedures for adhering to data breach notification laws or policies?</p>		<input type="checkbox"/>	<input type="checkbox"/>

Policy Review Checklist

			Annual Review Checklist		
Criteria not addressed	Not applicable (N/A)	Comments/Suggestions	Check if provision requires update	Was the provision revised?	Annual Review Comments
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	

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

Template Section	Policy Provision Checklist			
	Does the entity's privacy policy clearly state the following:	Page/section in policy	Criteria met	Criteria partially met
M. Information Retention and Destruction	<p>1. The entity's review schedule for validating or purging information?</p> <p>The periodic basis for this and/or reference to the applicable law(s)?</p> <p>Note: Retention and destruction policy should be provided for all information and intelligence databases/ records held by the entity.</p>		<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>
	<p>2. Whether the entity has a retention and destruction policy?</p> <p>Whether laws are referenced, if applicable?</p>		<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>
	<p>3. What methods the entity employs to remove or destroy information?</p>		<input type="checkbox"/>	<input type="checkbox"/>
	<p>4. Whether approval is needed prior to removal or destruction of information?</p> <p>Whether the law, statute, regulation, or policy that requires permission to be obtained before destroying information is cited, if applicable, or whether the policy specifies that no approval will be required?</p>		<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>
	<p>5. Whether the source of the information is notified by the entity prior to removal or destruction?</p>		<input type="checkbox"/>	<input type="checkbox"/>
	<p>6. Whether a record is kept of dates when information is to be removed (purged) if not validated prior to the end of its period?</p> <p>Whether notification is given prior to removal (for example, an autogenerated system prompt to entity personnel that a record is due for review and validation or purge)?</p>		<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>
<p>N. Accountability and Enforcement N.1 Information System Transparency</p>	<p>Information System Transparency</p> <p>1. Whether the entity's privacy policy is available to the public (for example, provided to the public for review, made available upon request, and posted on the entity's Web site—include Web address)?</p>		<input type="checkbox"/>	<input type="checkbox"/>

Policy Review Checklist

			Annual Review Checklist		
Criteria not addressed	Not applicable (N/A)	Comments/Suggestions	Check if provision requires update	Was the provision revised?	Annual Review Comments
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	

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

Template Section	Policy Provision Checklist			
	Does the entity's privacy policy clearly state the following:	Page/section in policy	Criteria met	Criteria partially met
	<p>2. Whether the entity has a point of contact (position/title) for handling inquiries or complaints?</p> <p>Whether the contact information for this individual (for example, phone, Web site, e-mail, or U.S. mail address) is provided?</p>		<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>
N.2 Accountability	Accountability			
	1. Whether electronic access (portal) to the entity's data identifies the user and whether the identity of the user is retained in the audit log?		<input type="checkbox"/>	<input type="checkbox"/>
	2. Whether a log is kept of accessed and disseminated entity-held data and whether an audit trail is maintained?		<input type="checkbox"/>	<input type="checkbox"/>
	3. The procedures and practices the entity follows to enable evaluation of user compliance with system requirements, the entity's privacy policy, and applicable law?		<input type="checkbox"/>	<input type="checkbox"/>
	4. Whether the entity has a mechanism for personnel to report errors and violations of entity policies related to protected information?		<input type="checkbox"/>	<input type="checkbox"/>
	5. Whether audits are completed by an independent third party or a designated representative of the entity?		<input type="checkbox"/>	<input type="checkbox"/>
	Whether the audits are conducted both annually (or other time period) and randomly?		<input type="checkbox"/>	<input type="checkbox"/>
N.3 Enforcement	Enforcement			
	1. The 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 the entity's privacy policy?		<input type="checkbox"/>	<input type="checkbox"/>
	2. 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?		<input type="checkbox"/>	<input type="checkbox"/>

Policy Review Checklist

				Annual Review Checklist		
Criteria not addressed	Not applicable (N/A)	Comments/Suggestions	Check if provision requires update	Was the provision revised?	Annual Review Comments	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No		
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No		
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No		
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No		
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No		
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No		
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No		
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No		
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No		
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No		
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No		
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No		

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

Template Section	Policy Provision Checklist			
	Does the entity's privacy policy clearly state the following:	Page/section in policy	Criteria met	Criteria partially met
O. Training	1. What personnel the entity requires to participate in training programs regarding implementation of and adherence to this privacy policy?		<input type="checkbox"/>	<input type="checkbox"/>
	2. Whether the entity provides training to personnel authorized to share protected information through the ISE?		<input type="checkbox"/>	<input type="checkbox"/>
	3. What is covered by the 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)?		<input type="checkbox"/>	<input type="checkbox"/>

Policy Review Checklist

			Annual Review Checklist		
Criteria not addressed	Not applicable (N/A)	Comments/Suggestions	Check if provision requires update	Was the provision revised?	Annual Review Comments
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	



rev. 9/8/11

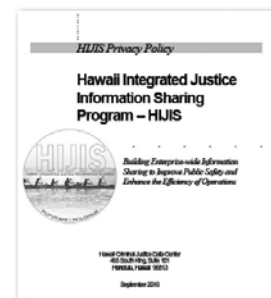
Appendix E—Sample Privacy Policies

To assist agencies in the policy drafting process, the following privacy policies are provided as reference samples within this appendix. Each policy was developed and customized using the recommendations in the *Privacy, Civil Rights, and Civil Liberties Policy Development Template for State, Local, and Tribal Justice Entities*, contained in Appendix C.1 of this Privacy Guide.

E.1 Hawaii Integrated Justice Information Sharing (HIJIS) Program



The Hawaii Integrated Justice Information Sharing (HIJIS) Program provides statewide services throughout Hawaii via a common architecture to securely and efficiently share appropriate information, both locally and nationally, for justice and nonjustice purposes, for improved public safety and homeland security, while respecting the privacy of citizens. The HIJIS Program is designed to build real-time information sharing in justice agencies throughout Hawaii in order to achieve greater efficiency, reduce duplicate data entry, speed the processing and access to justice information, and ensure that information is readily available and is accurate, timely and complete.



HIJIS is an information sharing framework that enables agencies to share information that is already collected and generated in their internal information systems as part of their daily business operations and enables authorized users to initiate a universal (or federated) query, constrained by the user's approved "right to know" and "need to know," to determine whether specific criminal justice information exists in other participating systems. In addition, the HIJIS framework enables automated notification to authorized persons or agencies of defined actions (e.g., the arrest of a person of interest or the change in their legal status).

Thanks to funding from the National Governors Association (NGA) Center for Best Practices'³⁴ Privacy Policy Academy, the attached privacy policy was developed for HIJIS' Proof of Concept using the *Privacy, Civil Rights, and Civil Liberties Policy Development Template for State, Local, and Tribal Justice Entities*, contained in Appendix C.1 of this Privacy Guide.

For more information on HIJIS, refer to www.hawaii.gov/hijis.

³⁴ National Governors Association (NGA) Center for Best Practices, www.nga.org/portal/site/nga/menuitem.50aee5ff70b817ae8ebb856a11010a0/.

HIJIS Privacy Policy

Purpose

The purpose of the Hawaii Integrated Justice Information Sharing (HIJIS) Privacy Policy is to describe how the principles of Freedom of Information and Right to Privacy, as defined in applicable Federal and State Law, will be applied in the context of the implementation of the HIJIS program.

The purpose of the HIJIS Privacy Policy is to ensure that the HIJIS program will respect and protect individual privacy and civil rights. The Privacy Policy aims to inform all involved in or affected by the collection and sharing of criminal justice information of their rights, duties, and limitations under this Policy.

Definitions

As used in this document, unless the context otherwise requires:

“Agency” means: any unit of government in this State, any county, or any combination of counties; department; institution; board; commission; district; council; bureau; office; governing authority; other instrumentality of state or county government; or corporation or other establishment owned, operated, or managed by or on behalf of this State or any county, but does not include the non-administrative functions of the courts of this State.

“Authorized user” means: a person, computer process, or device granted access to certain information, services, or functionality based on verified identity or credentials.

“Criminal justice information” means: information that may include criminal history records, case management information, deconfliction, conditions of supervision, case progress, wants and warrants, drivers records, identification, public records, and related justice information.

“Dissemination” means: the release, transfer, provision of access, sharing, publication, or divulging of a government record in any manner—electronic, verbal, or in writing.

“Government record” means: information maintained by an agency in written, auditory, visual, electronic, or other physical form.

“HIJIS” means: the Hawaii Integrated Justice Information Sharing Program.

“Need to know” means: 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, or homeland security activity, such as to further an investigation or meet another law enforcement requirement.

“Non-discrimination” means: religious, political or social views or activities, race, ethnicity, citizenship, place of origin, age, disability, gender, and sexual orientation will not be the sole basis for the collection and sharing of information on individuals.

“Non-justice purpose” means: the use of justice information for permitted purposes other than law enforcement or criminal justice, such as criminal background checks in connection with employment and licensing.

“Participating Agency” means: a justice or government agency participating in secure information sharing through HIJIS.

“Person” means: an individual, corporation, government, or governmental subdivision or agency, business trust, estate, trust, partnership, association, or any other legal entity.

“Personal record” means: any item, collection, or grouping of information about an individual that is maintained by an agency. It includes, but is not limited to, the individual’s education, financial, medical, or employment history, or items that contain or make reference to the individual’s name, identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

“Policy” means: this HIJIS Privacy Policy document.

“Privacy” means: freedom from unsanctioned intrusion. Refers to individuals’ interests in preventing the inappropriate collection, use, and release of personal information.

“Privacy Impact Assessment” or “PIA” means the methodology, and the resulting documentation, used by HIJIS to ensure that appropriate privacy measures are in place.

“Public” means: exposed to general view; accessible to or shared by all members of the community. (Merriam-Webster)

“Research and Analysis” means: the examination of criminal justice records for statistical classification or identification of relevant trends, not dependent on the identification of specific individuals associated with those records.

“Right to know” means: based on having legal authority or responsibility or pursuant to an authorized agreement, an agency or organization is authorized to access sensitive information and intelligence in the performance of a law enforcement, or homeland security activity.

“Security breach” means: an incident of unauthorized access to and acquisition of unencrypted or unredacted records or data containing personal information where illegal use of the personal information has occurred, or is reasonably likely to occur and that creates a risk of harm to a person.

Background

Legal Requirements

Information sharing capabilities of the Hawaii Integrated Justice Information Sharing Program (HIJIS), which enable participating agencies to access and share information through the HIJIS Framework, are subject to State and Federal laws governing the collection, use and dissemination of government and personal records. Principal among those laws are:

- Hawaii Revised Statutes (HRS) 92F (Uniform Information Practices Act),
- HRS 286-171 and 286-172 (Traffic Records),
- HRS 291C (Statewide Traffic Code),
- HRS 353 (Corrections),
- HRS 487J (Social Security Number Protection),
- HRS 487N (Security Breach of Personal Information),
- HRS 571 (Family Courts),
- HRS 846D (Juvenile Justice Information System), and
- Federal Code 28USC §534 (FBI Identification Records and Information).

Hawaii Administrative Rules also provide instruction to HIJIS participating agencies in the handling of government and personal records, creating additional context for the information exchanges enabled through HIJIS. Most immediately relevant are HAR Titles 8 (Department of Education) and 17 (Department of Human Services).

HIJIS will require that all participating agencies execute and maintain an information sharing Memorandum of Agreement (MOA)¹ in order to participate in the HIJIS program. The MOA will require participating agencies to distribute a printed copy of the Policy to their authorized users, who will acknowledge in writing receipt and compliance with the Policy. See Appendix A. for the text of the Memorandum of Agreement.

¹ HCJDC, Memorandum of Agreement for the Hawaii Integrated Justice Information Sharing Program, August 2008.

HIJIS Vision Statement²

The HIJIS Program envisions statewide services via a common architecture to securely and efficiently share appropriate information, both locally and nationally, for justice and non-justice purposes, for improved public safety and homeland security, while respecting the privacy of citizens.

HIJIS is not envisioned as a comprehensive, singular data warehouse that duplicates the information that agencies already capture and share, nor is it an all-encompassing system that each agency must adopt in lieu of their internal information systems. Rather, HIJIS is envisioned as an information sharing framework that will enable agencies to share information that is already collected and generated in their internal information systems as part of their daily business operations.

The HIJIS Framework will operate to electronically push and pull information between systems in accordance with rules that participating agencies develop and according to standards that will be adopted. HIJIS will enable authorized users to initiate a universal (or federated) query, constrained by the user's approved right to know and need to know, to determine whether specific criminal justice information exists in other participating systems. In addition, the Framework will enable automated notification to authorized persons or agencies of defined actions (e.g., the arrest of a person of interest or the change in their legal status).

Guiding Principles

The information in this section of the Policy is presented to describe the context of purpose and law that forms the foundation for HIJIS and the best practices for responsible sharing of criminal justice information. This context should serve as a foundation for the resolution of issues not otherwise specifically addressed in this Policy.

1. HIJIS:

The HIJIS Executive Committee and Operational and Technical Working Groups formulated a series of values which guide and direct the HIJIS planning effort.³

Among those values are the following with direct relevance to this Privacy Policy:

- Through integrated justice information sharing, HIJIS will improve public safety and homeland security, enhance the effectiveness of decision making and operations, and achieve greater efficiency and return on investment.
- The justice system should be fair to all parties, respecting the constitutional rights of defendants, and ensuring protection of the rights and privacy of victims and the public.
- HIJIS will provide services that contribute to public trust and confidence in the justice system.

2. Hawaii State Law:

Existing Hawaii laws and administrative regulations governing the collection, use, analysis, retention, destruction, and dissemination of government and personal records are applicable to HIJIS participating agencies individually, and to the information sharing capabilities of the HIJIS program. The Hawaii Uniform Information Practices Act (UIPA) noted that ". . . the legislature declares that it is the policy of this State that the formation and conduct of public policy--the discussions, deliberations, decisions, and action of government agencies--shall be conducted as openly as possible. The policy of conducting government business as openly as possible must be tempered by a recognition of the right of the people to privacy, as embodied in section 6 and section 7 of Article I of the Constitution of the State of Hawaii."⁴

UIPA describes restrictions to public inspection in an effort to balance individual privacy interests with the interests of the general public to access government information. It created the Office of Information Practices (OIP), which has published the Uniform Information Practices Act Reference Manual, containing advisory opinions and guidelines interpreting this chapter.

² HCJDC, *2008 Strategic Plan*, Hawaii Integrated Justice Information Sharing, December 2007.

³ *Ibid.*

⁴ HRS 92F-2.

Applicability

All organizations that participate as Participating Agencies in the HIJIS program, their staff, users, assigned technology support staff, and contractors, are subject to the provisions and requirements of this Policy. Participation includes sharing, contributing, or accessing information through the HIJIS Framework.

Other government agencies that contribute or obtain information through HIJIS are required to abide by the provisions and requirements of this policy as a condition of such information sharing.

This Policy recognizes and requires the existence of privacy policies within each Participating Agency, governing the collection, storage, dissemination, and destruction of criminal justice information by the agency. Such agency privacy policies will provide greater detail than this Policy and will include addressing legal requirements for the protection of privacy, civil rights, and civil liberties, and will, at minimum, be at least as comprehensive as the provisions contained within this HIJIS privacy policy. Participating agencies are guided to utilize the State and Local Privacy Policy Development: Privacy, Civil Rights, and Civil Liberties Policy Workbook in the development of their privacy policies to ensure agency policies are consistent throughout and that the policies meet all necessary privacy protection recommendations.

This Policy includes general information regarding the rights of individuals to access government records.

Policy

Where this Policy is in conflict with Federal, State, or Local law, the conflict should be brought to the attention of the HIJIS Executive Committee and this committee will update this Policy, as appropriate.

The information in this Policy aims to represent the principal intent of the referenced sections of state and federal law. It is provided in concise form to improve the communication of that intent. Of necessity, the representation of the applicable law sections will not be complete as to the nuances in the law. The references are provided to facilitate a complete understanding of the requirements of the applicable laws with respect to this Policy.

Information Collection

HIJIS operates as an information sharing framework that will enable participating agencies to access and share criminal justice information. HIJIS will not collect and store or retain information (except for information regarding users and uses of HIJIS required to ensure the security of HIJIS and the integrity of the data), but shall serve as the technical conduit through which such information shall be made available to authorized users for authorized purposes. All information collection and record storage will remain within the purview of the participating agencies, governed and controlled by legal statutes and administrative rules relevant to the functions and duties of the agencies and the purpose of the collection of information by the agencies.

HIJIS will implement best practices that will examine information exchanges for participating agencies' information collection methods, through the process of Privacy Impact Assessment (PIA, see below). Such methods are required to comply with applicable Federal, State and local law regarding nondiscriminatory and least-intrusive information collection practices.

Public Information Access

There are no plans at present to deploy HIJIS as a mechanism for the direct inspection and duplication of justice information by or for the general public. As a consequence, the HIJIS Privacy Policy will not address information privacy and protection aspects of access by the public to justice information. Members of the general public will be referred to the appropriate agency for permitted access to justice information. Participating agencies' privacy policies will be required to address privacy considerations and limitations on the dissemination of information retained by that agency. HIJIS is intended to provide information exchange between participating agencies only. Policy regarding such exchanges, which for purposes of this Privacy Policy is termed Information Sharing, is described below.

HIJIS will implement best practices that will examine information exchanges for information privacy compliance through the process of Privacy Impact Assessment (PIA, see below).

Information Analysis

HIJIS, as presently envisioned, does not offer the capability of sharing of criminal justice information for research and analysis purposes. The responsibility for providing such authorized access is directly assigned to the individual agencies that are the originating source of the data. Statutes addressing access to criminal justice information for research or statistical analysis purposes are specific regarding the circumstances and sources of authorization for such access.

Information Quality and Maintenance

1. Best Practices

Participating agencies shall establish procedures and processes to ensure and periodically review the quality (for example accurate, complete, current, verifiable, and reliable) of the information it collects, maintains, and shares through HIJIS.

2. Audits

HIJIS shall adopt technologies and procedures to ensure that all uses of the HIJIS Framework are authorized for official purposes, that all information which is shared through the HIJIS Framework is relevant and appropriate for such authorized uses, and that safeguards are in place to actively monitor and historically record the access and use of the HIJIS system, identifying authorized users and the nature of the information exchange.

Periodic audits of the use of the HIJIS Framework shall be conducted in order to maintain effective security, ensure privacy, and to assess ongoing operations. Such procedures shall also provide for the periodic review by HIJIS participating agencies of their applicable information collection, data quality assurance, storage, and sharing policies and procedures. The results of this review must reflect the name of the reviewer, date of review and explanation of relevant findings and recommendations. Audits shall be held as often as practicable, but at least every three years. Audits shall be performed by appropriate staff, to ensure that the audit will not expose privileged information to auditors not authorized to receive such information. Conduct of an audit, and the resulting issuance of findings and recommendations, shall be acknowledged in writing by the agencies participating in the audit.

3. Error Reporting (between participating agencies)

HIJIS shall adopt procedures to assure that participating agencies shall be informed of the need to correct or remove information that is erroneous, misleading, obsolete or otherwise unreliable.

The procedures shall require that the Participating Agency determining the need to correct or remove information inform the Consultative Center of Excellence (COE) staff of such a need. Upon determination of the source and scope of distribution of the information in question, COE staff will notify the source and all recipient agencies in writing, including electronic notification, of the incorrect or incomplete data. Agencies so notified, will be required to exercise the procedures in their Data Quality Assurance Policy promptly, to ensure the quality of the information exchanged.

4. Request for corrections by individuals

If an individual has complaints or objections to the accuracy or completeness of information about him or her, the individual will be referred to the agency originating the information. HIJIS Consultative COE staff will be notified by the agency receiving the complaint for follow up with the agency originating the information to determine disposition of the complaint and any need of follow-up as described in the previous section.

Information Sharing

1. Use HIJIS only

Participating agencies shall use only HIJIS for information sharing where feasible to ensure compliance with requirements of data privacy, security, and protection.

2. As authorized only

Information access and sharing between participating agencies through HIJIS is only permitted for authorized purposes, as defined by law, court order, or for business practices that are a necessary component of the requesting agency's duties and functions, and is compatible with the purpose and expectations of use under which the information was collected.

Authorized access will be determined in the context of the agency privacy policy governing the information system that is the source of the information to be exchanged. Implementation of restrictions on access based on the agency privacy policy within the context of HIJIS will be role-based.

3. Data labeling

HIJIS information exchanges will identify the source and other available descriptive labels of the information exchanged, where possible, to aid in recognizing restrictions in handling of information. At a minimum, the federated query and subscription/notification capabilities of HIJIS will feature such identification.

Federated query results will clearly identify search results that are only partial matches to the submitted selection criteria. Where feasible and meaningful, the query results may include a numeric indication of the degree of confidence in the accuracy of the partial match.

4. No mass dissemination

HIJIS will not provide bulk record dissemination. For purposes of properly authorized research and statistical analysis, such bulk dissemination shall be requested from the agency responsible for the collection and storage of the requested information.

5. No third party sharing (pass through)

Participating agencies shall not disseminate or share any information obtained or accessed through the HIJIS Framework to any other person, agency or organization. All HIJIS participating agencies shall use HIJIS for information dissemination where feasible to ensure compliance with requirements of data privacy, security, and protection.

If a non-participating agency requests information, that is exchanged through HIJIS between participating agencies, that non-participating agency shall request that information directly from the agency responsible for the collection and dissemination of such information.

6. PIA

HIJIS uses the Privacy Impact Assessment (PIA) as a method to examine and document the information privacy, security, and data protection policies, practices and procedures in use at agencies that apply to become participating agencies in HIJIS, or that wish to introduce new information exchanges into HIJIS.⁵ Agency privacy policies will be reviewed to ensure that they address the legal requirements for collection purposes and techniques, secure storage, data quality assurance and maintenance, permissible dissemination, and removal or destruction.

The PIA will examine policies within the subject agency regarding information sharing practices to non-participating agencies.

The PIA will identify areas of concern, and will allow suggestions for compliance with HIJIS requirements to be provided to the agencies. HIJIS will use the PIA as an aid in deciding to accept an agency or information exchange.

⁵ Kelly Peters and Eric Johnson, *Guide to Conducting Privacy Impact Assessments for State, Local, and Tribal Information Sharing Initiatives* (Washington, DC: U.S. Department of Justice, 2009).

Information Security

HIJIS shall adopt procedures to assure that the information exchanges between participating agencies are secure from unauthorized access, use or dissemination, 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. Access to information through HIJIS will be allowed only over secure networks. The participating agency 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.

Security measures and practices will be in accordance with the recommendations of the HIJIS Security Subcommittee.

The HIJIS Security Subcommittee is charged with providing recommendations for best practices and policy regarding data protection and security. Such recommendations are expected to also address matters of providing a secure environment and appropriate staff training. Once adopted, those recommendations will become part of this Policy.

Training

Participating agencies shall provide training for their staff, users, assigned technology support staff, and contractors regarding adherence to the provisions of this Policy and the agency's privacy policy.

The training program shall cover, as a minimum:

1. The purposes of the privacy policies
2. The substance and intent of the provisions of the privacy policies
3. The responsibilities and obligations of the agency under applicable law and policy
4. The implementation of the policies in day-to-day work
5. The impact of violations of the policies, and associated sanctions
6. The procedures for reporting violations of the policies.

Governance

The HIJIS Program is governed by an Executive Committee of agency executives and leaders, an Operational Working Group of agency managers and operational practitioners, and a Technical Working Group of technology experts responsible for building and operating the information technology assets of participating agencies.⁶

The HIJIS architecture document expands on the discussion of HIJIS governance found in the Strategic Plan and references a Consultative COE.⁷

The Department of the Attorney General has the overarching responsibility for the operation of the HIJIS Program.

Agencies are required to sign the HIJIS Memorandum of Agreement⁸ as condition of acceptance as a participant in HIJIS. The Memorandum of Agreement spells out the agency's responsibilities in adopting, supporting, and implementing policies, standards, and practices consistent with the goals of HIJIS.

The Privacy Policy Team created to draft this Policy will be responsible for review and update of the Policy every three years, or sooner as deemed necessary in response to changes in applicable law, technology, the purpose and use of the information systems, and public expectations. In affiliation with the Consultative COE, it will provide oversight and direction to the application of the PIA process, as described in this document. Participating agencies and the COE may request Policy review upon demonstrated need.

⁶ HCJDC, *2008 Strategic Plan*, Hawaii Integrated Justice Information Sharing, December 2007.

⁷ HCJDC, *HIJIS Architecture*, Version 1.0, March 27, 2009.

⁸ HCJDC, Memorandum of Agreement for the Hawaii Integrated Justice Information Sharing Program, August 2008.

Each Participating Agency will be required to designate an agency employee to be privacy policy compliance official, who will have responsibility to ensure agency adherence to the provisions of the Policy. This person will be the agency's liaison to the Privacy Policy Team, or its designee in the Consultative COE.

Questions, comments, or requests regarding this Policy and its provisions and requirements may be directed to the HIJIS Program Manager at the Hawaii Criminal Justice Data Center. The HIJIS Program Manager or designee will keep a record of such requests.

Accountability

Enforcement

Under the terms of the Memorandum of Agreement, participating agencies have made a commitment to implement internal business practices consistent with the strategic direction and goals of the HIJIS Program. Through this Policy, such business practices will include adherence to and enforcement of the provisions of the Policy.

Any time a participating agency becomes aware of a potential violation of the provisions of this Policy involving its information systems, staff, or practices, the agency will promptly investigate the nature and circumstances of the potential violation and institute any necessary corrective or remedial measures and sanctions.

If any participating agency or its staff has reason to believe a violation of the Policy has occurred, the agency's privacy compliance official will report relevant information to staff at the Consultative COE. If the violation took place at the reporting agency, its report will include its actual or proposed actions to correct the violation. If the reported potential violation took place at another participating agency Consultative COE staff will immediately inform the affected agency.

Consultative COE staff will be available to advise the affected agency regarding corrections, remedies, and sanctions appropriate for the violation. The agency's internal policies and procedures will be basis for any sanctions to be instituted.

At the conclusion of an instance of reported violation, the affected agency will submit a report of its actions to the Consultative COE.

Security Breach Notification

Any incident of unauthorized access to and acquisition of encrypted records or data containing personal or criminal justice information along with the confidential process or key constitutes a security breach.

Good faith acquisition of personal or criminal justice information by an employee or agent of an agency for a legitimate purpose is not a security breach; provided that the personal or criminal justice information is not used for a purpose other than a lawful purpose of the agency and is not subject to further unauthorized dissemination.

In accordance with State Law, any agency upon discovery of a security breach shall notify all affected individuals without unreasonable delay, subject to any delays requested by law enforcement agencies to support legal investigations or broader security concerns, and consistent with any immediate need to restore and ensure the integrity of any breached information system(s).

Such notice by the agency shall be clear and conspicuous and shall include a description of the following:

1. The incident in general terms
2. The type of personal or criminal justice information that was disclosed
3. How the personal or criminal justice information will be protected from further unauthorized dissemination
4. A telephone number and email address that can be called for further information and assistance
5. General advice on protection against identity theft that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.

Sanctions

Participating agencies are expected to enforce their respective privacy policies consistently and vigorously. Non-compliance with this Policy by a participating agency or its authorized users may result in suspension of access to the HIJIS program or other administrative sanctions, as recommended by the Executive Committee through the Privacy Policy Team or its designee in the COE.

A participating agency's privacy policy is required to clearly identify sanctions that may be instituted for violation of the agency's policy or this Policy.

Appendices

Memorandum of Agreement for the HIJIS Program

ARTICLE 1: INTRODUCTION

This Memorandum of Agreement (MOA) outlines a cooperative effort to support the development and implementation of the Hawaii Integrated Justice Information Sharing Program (HIJIS), and to jointly promote:

1. Efficient and expansive information sharing between justice, public safety, and other agencies at all levels of government,
2. Cost effective development and deployment of information systems,
3. Better quality decision making as a result of more timely, accurate and complete information, and
4. Enhanced public safety, homeland security and improved operations.

A. PARTICIPATING AGENCIES

The following agencies are parties to this MOA:

1. Department of the Attorney General
2. Honolulu Police Department
3. Kauai Police Department
4. Maui Police Department
5. Hawaii County Police Department
6. The Department of the Prosecuting Attorney, City and County of Honolulu
7. Office of the Prosecuting Attorney, County of Hawaii
8. The Department of the Prosecuting Attorney, County of Maui
9. Office of the Prosecuting Attorney, County of Kauai
10. The Judiciary
11. Department of Defense
12. Department of Public Safety
13. United States Attorney's Office, District of Hawaii

This MOA anticipates that future signatories (future parties) will become participating parties as described in ARTICLE 2.

B. PURPOSE

Justice and public safety agencies at state and local levels throughout Hawaii have a critical and enduring need to access and share information at every stage of the criminal justice process. Recognizing the need for broad access and automated sharing of critical information at key decision points throughout the justice and public safety enterprise, representatives of state and local justice and public safety agencies have come together to assess current operations and to create a vision and a plan for information sharing that will ensure public safety, enhance the quality of decision making, and increase the efficiency of operations while maintaining the privacy and confidentiality of information and the security of information systems.

The HIJIS Program is designed to build real-time, secure information sharing among justice and public safety agencies throughout Hawaii in order to achieve greater efficiency, eliminate or reduce duplicate data entry, speed the processing and access to justice information, improve decision making by ensuring that information is readily available, and that it is accurate, timely and complete. The HIJIS Strategic Plan was created to build a comprehensive blueprint for enterprise-wide information sharing among justice and public safety agencies.

The HIJIS Strategic Plan reflects an unprecedented collaboration of state and local justice and public safety officials, operational practitioners, and information technology experts. The plan establishes a foundation to guide continuing work in building a statewide information sharing infrastructure, expanding and enhancing operational information systems among participating agencies, defining information exchange standards and services, and improving business operations for effective decision making.

The purpose of this MOA is to formalize the relationship between HIJIS participating agencies in order to maximize cooperation and to promote effective government information sharing through collaborative decisionmaking, coordinated planning, and cooperative implementation among justice and public safety agencies and relevant partners for the fair, efficient, and effective operation of the justice system.

ARTICLE 2: GOVERNANCE

A. EXECUTIVE COMMITTEE

HIJIS is governed by an Executive Committee (EC) that is comprised of one representative of each of the signatory agencies (identified below). The EC sets policy and strategy, secures funding, and approves the HIJIS Strategic Plan and associated planning and implementation documents.

Membership on the EC is conditioned on:

1. Signing this MOA,
2. Actively participating in meetings, and
3. Providing resources in support of HIJIS planning and implementation.

The EC will meet as often as needed to successfully conduct business and at least semiannually. At any meeting of the EC a majority shall constitute a quorum. The EC will operate by consensus. If consensus on a particular issue is not possible, each participating party will have a single vote and decisions will be made by a simple majority of votes cast. The Chair of the EC will have the ability to break tie votes.

The EC will meet annually to review performance, set target outcomes for the coming year, and ensure provision of adequate resources. Participating agencies will identify a primary and an alternate person to represent the agencies on the EC. The agency head or designated representative will sign the MOA on behalf of the member agency, and either the primary or the alternate will represent the member agency on the EC and be empowered and instructed to conduct the EC's business.

The Hawaii Attorney General will serve as Chairperson of the EC and will perform the usual duties of a chairperson at such meetings. On occasions when the EC is to be officially represented, the Chairperson will be the representative, unless he/she designates some other member of the EC to serve in such capacity. The Chairperson may create any ad hoc committee for the EC as the Chairperson deems appropriate to the conduct of business.

The Hawaii Criminal Justice Data Center (HCJDC) will organize, facilitate, and document meetings of the EC and other committees and/or working groups authorized and created by the EC.

B. WORKING GROUPS

The EC will appoint an Operational Working Group and a Technical Working Group to assist in planning, research, development and implementation of the HIJIS Program.

The Operational Working Group will be comprised of operational practitioners at state and local levels across relevant participating agencies throughout Hawaii. The Working Group is responsible for organizing the vision established by the EC, defining operational requirements and business processes to realize that vision, and for providing insight and direction in developing a business plan for information sharing.

The Technical Working Group will be comprised of technical representatives of participating agencies and supporting IT offices. The Working Group is responsible for technical and infrastructure assessments, developing and adopting standards that will enable information sharing, researching and proposing technical solutions, pilot projects, and technical specifications in support of the HIJIS Program.

The EC may appoint additional Working Groups as necessary.

C. FUTURE PARTICIPATING PARTIES

Other governmental agencies may join the HIJIS Program and have representation on the EC provided:

1. Their participation is essential to effective information sharing for justice and public safety, and
2. They sign this MOA.

All requests to join HIJIS must be approved by majority vote of the EC. Once approved, future parties become fully participating parties and have all of the rights and obligations discussed herein.

ARTICLE 3: RESPONSIBILITIES

Participating agencies agree to:

1. Accept membership on the EC, responsibilities, policies and procedures associated with the HIJIS Program as described in this MOA.
2. Coordinate planning, design, development and implementation of internal agency information systems and business practices to be consistent with and in furtherance of the strategic direction and goals of the HIJIS Strategic Plan.
3. Adopt, support and implement information sharing standards that are jointly formulated and adopted as part of the HIJIS Program, and that will enable participating agencies to access and share relevant information, while respecting privacy rights, confidentiality of data, and security of systems.
4. Accept the HIJIS Privacy Policy as the governing document to direct participating agencies' practices and policies with respect to safeguarding privacy rights and confidentiality of data, and ensuring that each authorized HIJIS user in the agency acknowledges, in writing, receipt and compliance with the Privacy Policy.
5. Implement business practices that will ensure accurate, timely, and complete information collection and dissemination.
6. Provide support for the HIJIS Program through Executive Committee and Working Group participation, research and analysis of agency operations, and development of policies to achieve the aims of the HIJIS Program.

DURATION AND MODIFICATIONS

This MOA shall become effective upon execution and shall remain in effect until amended or terminated. This MOA may be modified at any time by written consent of all parties involved.

SIGNATORIES

The undersigned have read and signed this agreement on behalf of their agencies.

Executed this _____ day of _____, 2008:

Department of the Attorney General

Honolulu Police Department

Kauai Police Department

Maui Police Department

Hawaii County Police Department

The Department of the Prosecuting Attorney, City and County of Honolulu

Office of the Prosecuting Attorney, County of Hawaii

The Department of the Prosecuting Attorney, County of Maui

Office of the Prosecuting Attorney, County of Kauai

The Judiciary

Department of Defense

Department of Public Safety

United States Attorney’s Office, District of Hawaii

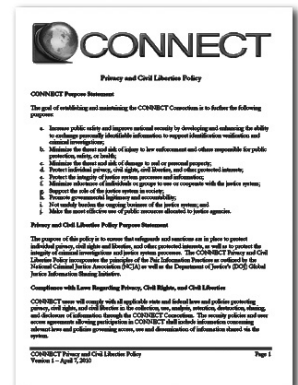
E.2 CONNECT

CONNECT is a consortium of states (founding members are Alabama, Kansas, Nebraska, and Wyoming) dedicated to working closely together to better solve specific information sharing challenges facing the criminal justice community. CONNECT provides a meaningful way for members to work together, pool limited resources, coordinate the creation and deployment of standards-based information sharing tools, and promote the sharing of information across jurisdictional borders to better solve and prevent crimes in their home communities.



The consortium consists of a structured way for each state's criminal justice information sharing organization to collaborate with their peers to solve specific information sharing challenges by leveraging the Global Justice Information Sharing Initiative (Global) standards.

CONNECT also gives value to the justice and public safety community by publishing lessons learned and sharing the CONNECT artifacts freely with practitioners nationwide.



Thanks to funding from the National Governors Association (NGA) Center for Best Practices³⁵ Privacy Policy Academy, the attached privacy policy was developed for CONNECT's Proof of Concept using the *Privacy, Civil Rights, and Civil Liberties Policy Development Template for State, Local, and Tribal Justice Entities*, contained in Appendix C.1 of this Privacy Guide. CONNECT is now in operation across the four-state federation, and its first data set, driver's license information, can be securely shared by authorized criminal justice officials in compliance with CONNECT and participating state privacy and operating policies.

For more information on CONNECT, refer to www.connectconsortium.org/. For information on CONNECT's bylaws, privacy policy, and member Privacy Impact Assessments, refer to www.connectconsortium.org/policy.cfm.

CONNECT Privacy and Civil Liberties Policy

CONNECT Purpose Statement

The goal of establishing and maintaining the CONNECT Consortium is to further the following purposes:

- a. Increase public safety and improve national security by developing and enhancing the ability to exchange personally identifiable information to support identification verification and criminal investigations;
- b. Minimize the threat and risk of injury to law enforcement and to law enforcement and others responsibility for public protection, safety, or health;
- c. Minimize the threat and risk of damage to real or personal property;
- d. Protect individual privacy, civil rights, civil liberties, and other protected interests;
- e. Protect the integrity of justice system process and information;
- f. Minimize reluctance of individuals or groups to use or cooperate with the justice system;
- g. Support the role of the justice system in society;
- h. Promote governmental legitimacy and accountability;
- i. Not unduly burden the ongoing business of the justice system; and
- j. Make the most effective use of public resources allocated to justice agencies.

³⁵ Ibid.

Privacy and Civil Liberties Policy Purpose Statement

The purpose of this policy is to ensure that safeguards and sanctions are in place to protect individual privacy, civil rights and liberties, and other protected interests, as well as to protect the integrity of criminal investigations and justice system processes. The CONNECT Privacy and Civil Liberties Policy incorporates the principles of the Fair Information Practices as outlined by the National Criminal Justice Association (NCJA) as well as the Department of Justice's (DOJ) Global Justice Information Sharing Initiative.

Compliance With Laws Regarding Privacy, Civil Rights, and Civil Liberties

CONNECT users will comply with all applicable state and federal laws and policies protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing, and disclosure of information through the CONNECT Consortium. The security policies and user access agreements allowing participation in CONNECT shall include information concerning relevant laws and policies governing access, use and dissemination of information shared via the system.

Prior to granting an individual user access to CONNECT, the CONNECT Member shall ensure that each user within its state acknowledges receipt of this policy and agrees to comply with the terms of this policy.

Each CONNECT Member shall provide the CONNECT Board with documentation relative to their internal operating policies related to privacy and security prior to being granted access to CONNECT. This documentation must demonstrate that the CONNECT Member policies are in compliance with applicable laws protecting privacy, civil rights and civil liberties.

Prior to allowing users to access CONNECT, each CONNECT Member shall establish an automated method (e.g. pop-up window or notification method) to periodically remind users that unauthorized access to CONNECT is prohibited. Users will have to acknowledge receipt of this warning prior to being allowed to proceed with any queries of the system (e.g. by checking an onscreen box or otherwise acknowledging receipt of the message.) Each CONNECT Member shall provide a hyperlink to a full copy of this policy to all users accessing CONNECT.

Governance and Oversight

CONNECT affairs are led by a Board. Each Member of the CONNECT consortium shall appoint one Representative to serve on the Board. The activities of the CONNECT Board are governed by the CONNECT Bylaws, a copy of which is available on www.connectconsortium.org.

Each CONNECT Member shall designate a privacy point of contact. The CONNECT Consortium public website shall maintain a form to receive complaints of misuse or suspected inaccuracies associated with data transmitted and received via CONNECT. A submission through this form shall be reviewed by the CONNECT Board Chair who will direct the reported misuse or inaccuracy to the CONNECT privacy point of contact in the state from which the data in question originated.

Any CONNECT user or member of the public who discovers potential errors or misuse may initiate a request for review via the form at www.connectconsortium.org. All requests for review will be investigated as soon as practicable by the CONNECT privacy point of contact in the state where the suspected inaccuracy occurred and/or where the alleged misuse occurred. Further, the request for review will be added as an agenda item for the next CONNECT Board meeting. Requestors will receive an email notification as soon as the privacy point of contact is notified of the suspected inaccuracy or alleged misuse. In addition, the requestor will be notified by the privacy point of contact of any corrective action taken once the matter has been fully investigated. In the event it is determined no corrective action is necessary, the requestor will be advised of this finding as well. All confirmed incidents of inaccurate data or misuse must be reported to the CONNECT Board.

If the originating CONNECT Member determines the misuse threatens the physical, reputational, or financial harm of a person or violates a statute requiring notice in the jurisdiction of that Member, that CONNECT Member shall take appropriate action to notify the individual about whom personal information was or is reasonably believed to have been breached or obtained. The notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or any measures necessary to determine the scope of the release of information and, if necessary, to reasonably restore the integrity of any information system affected by this release.

The CONNECT Board will produce an annual report which will be posted to the CONNECT website. The report shall include:

- Number of CONNECT users within each state;
- Number of CONNECT searches performed;
- Number of data quality complaints received;
- Number of corrections made based on complaints received;
- Number of allegations of misuse reported;
- Number of investigations completed;
- Number of persons receiving administrative sanctions for misuse of CONNECT; and
- Number of persons facing criminal charges for misuse of CONNECT.

The CONNECT Board will be responsible for the development and review of the CONNECT Privacy and Civil Liberties Policy. The CONNECT Board will review and update the provisions contained within the CONNECT Privacy and Civil Liberties Policy annually or upon the addition of data sets.

Requirements Regarding Information Gathered and Shared

Individual CONNECT Members will adopt policies and procedures requiring its users to:

- a. Only seek or retain information that is legally permissible for the agency to seek or retain under laws applicable to the originating agency;
- b. Only use lawful means to seek information;
- c. Only seek and retain information that is reliably accurate, current, and complete, including the complete, relevant context;
- d. Investigate in a timely manner any alleged errors and correct or delete information found to be erroneous;
- e. Retain information sought or received only so long as it is relevant and timely, and delete or return information that is inaccurate, outdated, or otherwise no longer related to known or suspected criminal activities;
- f. Maintain information and systems containing information in a physically and electronically secure environment and protected from natural or man-made disasters or intrusions;
- g. Engage in collation and analysis of information in a manner that conforms to laws and administrative rules and regulations applicable to CONNECT Members;
- h. Only allow authorized users to access the information in the shared system and only for purposes related to the performance of their official duties;
- i. Provide training to users concerning the CONNECT Privacy and Civil Liberties Policy and the impact of misuse of CONNECT and penalties to violations of this privacy policy and relevant state and federal laws and policies governing access to data;
- j. Maintain an activity log of information accessed or requested from CONNECT; and
- k. Establish and comply with information retention and destruction schedules where such exists.

Restrictions to User Access and Security Safeguards

The CONNECT Board requires each participating CONNECT Member to establish procedures, practices and protocols as well as use software, information technology tools and physical security measures to ensure information is accessed only by authorized personnel, and is protected from unauthorized access, modifications, theft or sabotage, whether internal or external or disasters or intrusions by natural or human causes.

Participating CONNECT Members shall confirm that they have credentialed, role-based levels of access and permissions. Each CONNECT Member shall establish a procedure for adding, maintaining and removing user accounts that uniquely identify individual users.

Information acquired or received through CONNECT by a user shall only be used for authorized criminal justice purposes as stated within this policy.

Any CONNECT risk and vulnerability assessment shall not be disclosed to the public.

Users may not confirm the existence or nonexistence of specific records contained within CONNECT to persons who are ineligible to receive information. However, general information concerning data sources and data elements available through CONNECT will be available on the public CONNECT website. Statutes governing the use of data pertaining to the source of the data provider will be posted to the CONNECT web site.

Sharing Information With Non-CONNECT Users

CONNECT information shall be made available to non-CONNECT users only in compliance with statutes and rules governing the originating CONNECT Member.

Disclosure of Information According to the Originating Agency's Access Rules

A participating agency will not disclose or otherwise use information originating from another CONNECT state except as authorized or required by law in the jurisdiction in which the information originated.

Description of Information to Be Shared

Users shall not seek or retain information about individuals solely based on their religious, political, or social views or activities; their participation in a lawful event; or their race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation.

CONNECT shall not be used to transmit data subject to the terms of 28 CFR Part 23.

CONNECT makes no claims concerning the usability or quality of the information exchanged via CONNECT. Any suspected errors or inaccuracies shall be reported to the CONNECT Member in the jurisdiction where the error was discovered. The CONNECT Member shall contact the originating CONNECT Member who has the responsibility to take appropriate steps as deemed necessary to correct the problem.

The public CONNECT website will provide contact information for each CONNECT Member. CONNECT Members must have a redress procedure established prior to contributing data.

No information received through CONNECT may be provided to commercial database providers.

CONNECT Members shall take appropriate measures to protect confidential sources and police undercover techniques and methods and to not interfere with or compromise pending criminal investigations.

Each CONNECT Information Exchange Package Documentation (IEPD) contains requirements concerning how contributing agencies shall specify metadata concerning records exchanged. The IEPD may be found at www.niem.org or www.it.ojp.gov. Specific information concerning data shared via CONNECT is available at www.connectconsortium.org.

Retention Policy

In the event information obtained via CONNECT becomes part of a criminal justice file, then the information entered into the file shall be retained in accordance with the recipient state's records disposition laws, policies and procedures governing the destruction of criminal justice records. Agencies are not required to give notice of records destroyed in accordance with their state's records disposition laws, policies and procedures.

Expectations Regarding Accountability, Enforcement and Sanctions

Each CONNECT Member must be able to generate computerized logs of all queries performed by users under their authority accessing CONNECT data via their portal.

CONNECT Members shall make a reasonable attempt to cooperate with audits by other CONNECT Members. These may be conducted as “mail-in” audits wherein one Member can request paper documentation of searches performed against their database(s) via CONNECT.

Each CONNECT Member shall conduct periodic random audits of queries and search returns performed by users within their jurisdiction through CONNECT.

Each CONNECT Member must ensure that users under their authority who have violated the terms of the CONNECT Privacy and Civil Liberties Policy are subjected to appropriate sanctions.

Enforcement of Provisions of Information Sharing Agreement

If a CONNECT Member fails to comply with the provisions of the CONNECT Privacy and Civil Liberties Policy, the CONNECT Board may impose sanctions according to its bylaws.

