United States
Department of Justice

Privacy, Civil Rights, and Civil Liberties

Policy Templates for Justice Information Systems

Privacy, Civil Rights, and Civil Liberties Policy Templates for Justice Information Systems

February 2008

About Global

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

BJA

This project was supported by Grant No. 2005-NC-BX-K164 awarded by the Bureau of Justice Assistance, in collaboration with the U.S. Department of Justice's Global Justice Information Sharing Initiative. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the U.S. Department of Justice.

Table of Contents

Acknowledgements

***P**rivacy, Civil Rights, and Civil Liberties Policy Templates for Justice Information Systems* is a product of the U.S. Department of Justice's (DOJ) Gloval Justice Information Sharing Initiative (Global) and was developed with the assistance of two of Global's working groups and individuals from several organizations and in partnership with the Justice Management Institute (JMI).

The policy templates presented here were drafted based on the shared wisdom, experiences, and comments of the justice practitioners and industry professionals who were members of the Global Intelligence Working Group and the Global Privacy and Information Quality Working Group. A special thank-you is expressed to the members of these two working groups and to Alan Carlson for contributing to and supporting this document.

Members of the Global Intelligence Working Group

Jack Anderson
Orange County Sheriff's Department
Norwalk, California

Maureen Baginski
Federal Bureau of Investigation
Washington, DC (retired)

William Berger
North Miami Beach, Florida, Police Department
Miami, Florida

Kenneth Bouche
Illinois State Police
Chicago, Illinois

Donald Brackman
National White Collar Crime Center
Richmond, Virginia

Ledra Brady
U.S. Drug Enforcement Administration
Quantico, Virginia (retired)

Ron Brooks
Northern California HIDTA
San Francisco, California

Melvin Carraway
Indiana State Police
Indianapolis, Indiana
(No longer a member)

Steve Casteel
U.S. Drug Enforcement Administration
Arlington, Virginia

Henry Coffman
INTERPOL-USNCB
Washington, DC

Carlo Cudio
Monterey Police Department
Monterey, California

Michael Duffy
U.S. Department of Justice
Washington, DC

Edward Flynn
Massachusetts Executive Office of Public Safety
Boston, Massachusetts

Max Fratoddi
Federal Bureau of Investigation
Washington, DC (retired)

Thomas Frazier
Major Cities Chiefs Association
Baltimore, Maryland

Dennis Garrett
Arizona Department of Public Safety
Phoenix, Arizona (retired)

Bart R. Johnson
New York State Police
Albany, New York

Vernon Keenan
Georgia Bureau of Investigation
Decatur, Georgia

Phil Keith
Knoxville Police Department
Knoxville, Tennessee (retired)

Gerard P. Lynch
Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network
Newtown, Pennsylvania
(Now Chief Executive Officer of Regional Information Sharing Systems® (RISS))

George P. March
Office of Information Technology
RISS
Thorndale, Pennsylvania

Ritchie Martinez
Arizona Department of Public Safety
HIDTA
Tucson, Arizona

Jerry Marynik
California Department of Justice
Sacramento, California

Miles Matthews
Counterdrug Intelligence Executive Secretariat
U.S. Department of Justice
Washington, DC
(No longer a member)

Kent Mawyer
Texas Department of Public Safety
Austin, Texas

Patrick McCreary
Bureau of Justice Assistance
Washington, DC

Peter Modafferi
Rockland County District Attorney's Office
New City, New York

Dennis Morton
National Drug Intelligence Center
Johnstown, Pennsylvania (retired)

Daniel Oates
Aurora Police Department
Aurora, Colorado

Thomas O'Connor
Maryland Heights Police Department
Maryland Heights, Missouri

Marilyn Peterson
New Jersey Division of Criminal Justice
Trenton, New Jersey (retired)

Joseph Polisar
Garden Grove Police Department
Garden Grove, California

Russ Porter
Iowa Department of Public Safety
Des Moines, Iowa

Louis Quijas
Federal Bureau of Investigation
Washington, DC

Richard Randall
Kendall County Sheriff's Office
Yorkville, Illinois

Steven Raubenolt
Office of the Attorney General
Columbus, Ohio

Edward Reina
Yavapai-Prescott Tribal Police Department
Prescott, Arizona

Richard Russell
U.S. Department of Homeland Security
Washington, DC
(Now with the ODNI)

Kurt Schmidt
Office of National Drug Control Policy
Washington, DC

Michael Schrunk
Multnomah County District Attorney's Office
Portland, Oregon

Richard Stanek
Minneapolis Police Department
Minneapolis, Minnesota

Gregory Stieber
U.S. Secret Service
U.S. Department of Homeland Security
Washington, DC
(No longer a member)

Mark Zadra
Florida Department of Law Enforcement
Tallahassee, Florida

Members of the Global Privacy and Information Quality Working Group

Francis X. Aumand III
Vermont Department of Public Safety
Waterbury, Vermont

Robert P. Boehmer
Institute for Public Safety Partnerships
University of Illinois at Chicago
Chicago, Illinois

David Byers
Arizona Supreme Court
Phoenix, Arizona

Alan Carlson
The Justice Management Institute
Kensington, California

Steven Correll
Nlets—The International Justice and Public Safety Network
Phoenix, Arizona

Cabell Cropper
National Criminal Justice Association
Washington, DC

Robert Deyling
Administrative Office of the United States Courts
Washington, DC

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

Bob Greeves
Bureau of Justice Assistance
Washington, DC

Barbara Hurst
Rhode Island Office of the Public Defender
Providence, Rhode Island

John Jesernik
Illinois State Police
Joliet, Illinois

Rhonda Jones
National Institute of Justice
Washington, DC

Erin Kenneally
San Diego Supercomputer Center
La Jolla, California

Erin Lee
National Governors Association
Washington, DC

Hayes Lewis
American Indian Development Associates
Albuquerque, New Mexico

Thomas MacLellan
National Governors Association
Washington, DC

Ada Pecos Melton
American Indian Development Associates
Albuquerque, New Mexico

Wil Nagel
Illinois Criminal Justice Information Authority
Chicago, Illinois

Jeanette Plante
Office of Records Management Policy
Justice Management Division
U.S. Department of Justice
Washington, DC

Michael Ramage
Florida Department of Law Enforcement
Tallahassee, Florida

Anne Seymour
Justice Solutions, Inc.
Washington, DC

Steve Siegel
Denver District Attorney's Office
Denver, Colorado

Cindy Southworth
National Network to End Domestic Violence Fund
Washington, DC

Martha Steketee
Independent Consultant
Chicago, Illinois

Elizabeth Whitaker
Georgia Tech Research Institute
Atlanta, Georgia

Carl Wicklund
American Probation and Parole Association
Lexington, Kentucky

Preface

Quite simply, privacy may be one of the most important issues affecting the use of technology in the twenty-first century. Responsively, the U.S. Department of Justice (DOJ), Office of Justice Programs, Bureau of Justice Assistance (BJA), is pursuing the best resources and recommendations from the field to further efficient, comprehensive, and appropriate sharing of information. These goals will be achieved by ensuring privacy and security protections are in place throughout the information exchange process, safeguarding the safety, health, and personal data of our nation's residents in the face of ever-advancing technologies.

A primary approach that BJA uses to explore key information sharing issues such as privacy and civil liberties (and arrives at associated recommendations) is through efforts of DOJ's Global Justice Information Sharing Initiative (Global) Advisory Committee (GAC or "Committee"). The GAC is a volunteer group of high-level justice executives and practitioners representing over 30 key agencies across the justice and public safety landscape (and, by extension, 1.2 million justice practitioners). This group serves as the Federal Advisory Committee to the highest-ranking law enforcement official in the land, the U.S. Attorney General, on standards-based justice-related information sharing.

GAC-supported recommendations and resources are informed through a number of avenues: mainly via the work of the Global working groups but sometimes (as in this case) as a result of subject-matter experts' activities. Recognizing the need for a hands-on privacy policy tool, the Justice Management Institute (JMI) diligently pursued the crafting of *Privacy, Civil Rights, and Civil Liberties Policy Templates for Justice Information Systems* ("templates"). When the JMI templates were presented to the GAC for review and discussion, Global members enthusiastically recognized their value to the field. Subsequently, the templates were included in the Committee's catalogue of "recognized resources."

BJA and the GAC strive to coordinate product development complementarily, with individual products proving useful both on their own as well as when viewed as a suite of tools. Considering that approach, please see Appendix Three: Bibliography for Sources and References for additional information sharing-related resource suggestions (most are also referenced in the body of this document). The enumerated Global items as well as other valuable DOJ-supported tools are available on the OJP Information Technology Initiatives Web site, located at http://it.ojp.gov. This appendix contains more information on the site and Global offerings.

Introduction

The atrocities of September 11, 2001, brought into focus the need to greatly improve our methods of gathering and sharing information on terrorists, criminal activities, and the individuals and organizations likely involved. It also highlighted the need to do so in an efficient manner, one that did not waste time and resources gathering irrelevant information, duplicating information already collected, or gathering information about people unlikely to be involved in illegal activities. Improving these capabilities would also enhance public confidence in the ability of the justice and public safety systems to protect people, property and, ultimately, our way of life. There are a number of aspects to improving our capacity to prevent harm, including taking advantage of new technology, making better use of existing technologies and systems, linking information systems, and improving our justice system policies and business practices.

One element of a more robust information gathering and sharing system is an up-to-date and comprehensive policy protecting individuals' privacy, civil rights, and civil liberties. Improved public safety does not have to come at the expense of these rights. Rather, public safety is further enhanced when individuals are sufficiently comfortable with the integrity of justice information system operations and therefore are willing to cooperate with and support them. Precisely drawn privacy, civil rights, and civil liberties protection policies thus contribute to a number of goals. First, such policies are legally required by the U.S. Constitution and state constitutions and other laws adopted over time that regulate life in our society and the operation of our public agencies. Second, a strong privacy policy is good public policy, because it is responsive to widely held public expectations about the collection and use of information about individuals and the fair and open operation of a democratic government. Third, it is the right thing to do.

Answering a Critical Need, Responding to the Field

The need for effective privacy policies has been consistently recognized in recent U.S. Department of Justice's (DOJ) Global Justice Information Sharing Initiative (Global) efforts (detailed in the Preface) directed at the improvement of justice information gathering and sharing systems:

- It is succinctly summarized in *Privacy, Civil Liberties, and Information Quality Policy Development for the Justice Decision Maker*;[1]
- It is supported by several recommendations of the *National Criminal Intelligence Sharing Plan* (NCISP),[2] and in response to a tremendous amount of requests from the field for assistance with the underlying process, the *Privacy and Civil Liberties Policy Development Guide and Implementation Templates*[3] was assembled.

Building on these previous works and offering excellent supplementation to the Global Policy Guide, the objective of *Privacy, Civil Rights, and Civil Liberties Policy Templates for Justice Information Systems* ("policy templates" or "templates") is to provide policy templates that justice system practitioners can use to draft comprehensive policies to protect privacy, civil rights, and civil liberties principles applicable to their operations.

Audience

The policy templates were developed for use by law enforcement agencies, prosecutors, courts, or other justice system agencies or jurisdictions at the local, state, regional, tribal, territorial, or federal level. The templates were designed to cover a range of computer-based justice information systems, including:

---

1 Located at http://it.ojp.gov/documents/global_privacy_brief.pdf.
2 Located at http://it.ojp.gov/documents/ncisp/. Note: High bandwidth required.
3 Located at http://it.ojp.gov/documents/Privacy_Guide_Final.pdf.

- An incident- or event-based records management system (RMS);
- An offender-based information system (OBIS) or offender-based tracking system (OBTS);
- A case management system (CMS) used by an agency or court;
- An integrated criminal justice information system (often referred to as IJIS or CJIS) supporting the activities of several agencies and related courts;
- A criminal history record information (CHRI) system;
- A criminal intelligence gathering system (CIS);
- A corrections or jail management system (JMS); or
- A justice information sharing network through which information in one or more of the above systems is shared with users of all systems involved.

The policy templates are intended for systems that seek or receive, store, and make available information in support of activities associated with the justice system, public safety, and health communities. These include criminal investigations, crime analysis, law enforcement, prosecution, defense, courts, corrections, pretrial services, probation, parole, or other activities in support of the protection of public safety, health, or other matters handled through the justice system. Also included are prosecution of activities or circumstances involving violations of public health and safety laws, including zoning and environmental protection. The templates are relevant to the administration of justice, strategic and tactical operations, and national security responsibilities. Finally, the templates are intended to address all types of public safety and public protection risks and threats, whether criminal or from natural disasters.

Scope of Policy Templates

The policy templates proposed here are intended to protect more than just individual privacy. The templates are more comprehensive, addressing:

- Protection of ***privacy***;
- Protection of ***civil rights***;
- Protection of ***civil liberties***; and
- ***Information quality***, which enhances the above protections.

As used in these policy templates, key terms are defined as follows:

> "The term ***privacy*** refers to individuals' interests in preventing the inappropriate collection, use, and release of personally identifiable information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. The U.S. Constitution does not explicitly use the word *privacy*, but several of its provisions protect different aspects of this fundamental right. Although there does not exist an explicit federal constitutional right to an individual's privacy, privacy rights have been articulated in limited contexts by the U.S. Supreme Court. [*Note: several state constitutions do contain explicit language regarding a right to privacy.*] Privacy protections are numerous and include protection from unnecessary or unauthorized collection of personal information (e.g., eavesdropping), public disclosure of private facts, and shame or humiliation caused by release of personal information." (*National Criminal Intelligence Sharing Plan* [NCISP], p. 6, emphasis added, footnotes omitted, and note addressing state constitutions added.)

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

civil rights involves positive (or affirmative) government action, while the term *civil liberties* involves restrictions on government." (NCISP, pp. 5–6, emphasis added.)

"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 . . . ." (NCISP, p. 5, emphasis added.)

Most state constitutions contain a statement of rights very similar to and sometimes broader than the Bill of Rights in the U.S. Constitution. It should also be noted that the Bill of Rights enumerated in the U.S. Constitution does not apply to American Indians when they are within Indian Country, although they are afforded the same protections under the Indian Civil Rights Act of 1968.

Information quality refers to various aspects of the information itself. Traditionally, the basic elements of information quality have been identified as accuracy, completeness, currency, reliability, and context/meaning. Today, information quality is being more fully described in multidimensional models, expanding conventional views of the topic to include considerations of accessibility, security,[4] and privacy. The issue of information quality is addressed more specifically in Section B.5.00 of this document. Readers wishing to further pursue the multidimensional aspect of the topic are encouraged to review Global's *Information Quality: The Foundation for Justice Decision Making*.[5]

While these templates address privacy, civil rights, and civil liberties, a review of the Table of Contents reveals sections addressing disclosure, public access, records retention, security, and data management issues.

- *Disclosure* is a subset of privacy, focusing on information that may be available only to certain people for certain purposes but which is not available to everyone.
- *Public access* relates to what information can be seen by the public, that is, information whose public availability is not subject to privacy interests or rights.
- Controlling who has access to information, whether public or internal, is one goal of *security provisions*.
- If information is not retained any longer than necessary under applicable *records retention* schedules, then there is no risk of improper disclosure after the records have been destroyed.

References to these topics are included in order to highlight the intersection of privacy, civil rights, and civil liberties interests with these operational aspects of justice system information sharing and management and because all the topics have implications for the protection of privacy, civil rights, and civil liberties.

Purpose of the Templates

It is important to understand what the policy templates are intended to do.

Existing federal and state constitutional provisions, statutes, rules, and regulations forbid certain conduct and prescribe what and how information can be collected. However, there are often gaps in these provisions—areas where agencies and individuals can exercise discretion about what to do or how to proceed. Agencies should consider adopting policies or practices regarding this discretion to provide more comprehensive protection of personal privacy, civil rights, and civil

[4] Please see Global's *Applying Security Practices to Justice Information Sharing* for more information on this topic. The resource is located at http://it.ojp.gov/documents/asp/. Note: High bandwidth required.

[5] Located at http://it.ojp.gov/documents/IQ_Fact_Sheet_Final.pdf.

liberties. One objective of these templates, therefore, is to both identify and organize applicable laws and to indicate where an agency might need to consider adopting new or additional policies or practices.

Concepts Underlying Templates

These proposed policy templates are based on several fundamental concepts intended to improve the effectiveness and success of the justice information systems being developed. These basic concepts include:

- Supporting a proactive approach to managing the collection, use, analysis, retention, destruction, sharing, and disclosure of information.
- Making decisions that are deliberate and considered when collecting or receiving, using, analyzing, retaining, destroying, sharing, and disclosing information.
- Reinforcing appropriate conduct of individuals in the collection, use, analysis, retention, destruction, sharing, and disclosure of information that complies with applicable local, state, regional, tribal, territorial, and federal laws.
- Proposing policy language that is relevant to all levels of government—local, state, regional, tribal, territorial, and federal.

Organization of Policy Templates

The policy templates proposed here are designed for use by any one of several types of information gathering or sharing systems described in the Audience section. In order to accommodate all of the common approaches, three sets of policy template provisions are provided in this document:

1. Privacy and civil rights protection provisions for inclusion in enabling legislation or authorization for the justice information system (Part A);
2. A basic privacy and civil rights protection policy template covering the day-to-day operation of the justice information system (Part B); and
3. Privacy and civil rights protection provisions for an interagency agreement[6] between agencies participating in a justice information sharing network or system through which each participating agency will share information (Part C). One provision of the agreement would be that each of the participating agencies will have a basic privacy and civil liberties policy that contains provisions addressing the policies identified in Part B.

Each of the several common approaches of justice information systems[7] would require use of a different combination of the three policy parts contained in this template:

- **Local systems** that serve one agency or the agencies and courts of a city, county, or tribe should include policy elements in their enabling legislation (Part A) and adopt the basic policy (Part B). If the local system joined an information sharing system, an interagency agreement would be needed regarding the participation in the sharing system (Part C).
- **Statewide systems** that provide one of the several types of justice information systems for any agency in the state choosing to use it would need all three policy elements: enabling authority (Part A), a basic policy for the operation of the system (Part B), and an interagency agreement (Part C) signed by each participating agency.

---

[6] Such agreements are referred to by a range of acronyms, depending on the state or type of agreement. Examples include IAA (Inter-Agency Agreement), JPA (Joint Powers Agreement), MOA (Memorandum of Agreement), or MOU (Memorandum of Understanding). In this document, "interagency agreement" is used as representative of all these terms.

[7] For descriptions of four frequently used justice information systems models, see Chapter 3 of Global's *Applying Security Practices to Justice Information Sharing*, located at http://it.ojp.gov/documents/asp/. Note: High bandwidth required.

- **A statewide network that integrates local systems** would need enabling legislation for the state-level system (Part A) and an interagency agreement with the participating agency systems (Part C).
- **Multijurisdictional information sharing systems** would need enabling authorization to establish the system (Part A) and an interagency agreement with the participating agencies (Part C). Regional systems could involve multiple jurisdictions across state lines, multiple jurisdictions within a state, or a combination of local, state, regional, tribal, territorial, and federal justice system agencies.
- **Ad hoc systems** that are created in response to an incident or event and will rely on existing information systems in the participating agencies would need an interagency agreement (Part C) tailored to the incident or event.

Format of Policy Templates

The policy templates proposed here contain two types of provisions.

1. There is language reflecting common practices. These are provisions that are straightforward and less controversial in nature, common across many states or across jurisdictions within a state or that incorporate federal provisions applicable to everyone.
2. There are provisions that typically are different in each local or state jurisdiction or where a local or state jurisdiction has unique or special requirements or limitations. These provisions must be tailored or augmented to reflect the specific local or state laws or practices. For these types of provisions, the templates include either alternate versions of common local or state policies or a statement in brackets indicating where local or state laws must be reviewed and reflected in the policy language. Examples include state constitutional or statutory provisions on what records are open to the public, limitations on what information can be sought or received, what methods can or cannot be used to seek or receive information, and records retention schedules.

Definitions of terms with a specific meaning in the policy templates are provided. These may need to be revised to reflect local definitions or terminology. Additional definitions may also need to be added for terms or phrases commonly used in a jurisdiction. Additionally, Appendix E of the *Privacy and Civil Liberties Policy Development Guide and Implementation Templates*[8] contains a glossary of terms and definitions readers may find helpful.

The proposed policy provisions are composed of three segments.

1. Each section begins with the actual policy language, the so-called "black-letter" language. This language is in bold type. It may include language that must be tailored to a jurisdiction's laws, noted in bold and italics within [brackets]. There may also be suggested additional provisions, also in bold and italics within [brackets].
2. Following the specific policy language is a Commentary segment that explains the meaning and intent of the black-letter language. The Commentary is in italics. The Commentary language would generally not be included in a policy but might be relevant to interpretations of the policy language once it is adopted and in use.
3. Finally, Appendix Five contains source and reference information for the language or concepts in each of the proposed sections. These include references to local, state, or federal statutes, regulations, or existing policies protecting privacy, civil rights, and civil liberties. There are also references to the relevant provisions from the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* promulgated by the European Organisation for Economic Co-operation and Development (OECD) and the Safe Harbor Privacy Principles developed by the U.S. Department of Commerce for compliance by U.S. companies with the OECD provisions. These are included because of the frequent reference to them in the field, although it must be noted that these provisions reflect European views of privacy, which are narrower than American views, and that the OECD Guidelines include a very broad law enforcement exception.

[8] Located at http://it.ojp.gov/documents/Privacy_Guide_Final.pdf.

How to Use the Templates

The policy templates provided here are designed to provide both a framework for and the language of provisions to be included in enabling legislation, an operations policy, or an agreement between two or more governmental agencies (hereafter referred to as an interagency agreement). They cover the privacy, civil rights, and civil liberties sections that would be incorporated into a larger document containing other provisions regarding the establishment and operation of a justice information system. The intention is for the templates to be used as follows:

- The sections in Part A regarding the enabling authority would be included in the statute, ordinance, resolution, executive order, or other document that authorizes or creates the entity that will oversee the information system.
- The sections in Part B regarding basic system operation would be part of a general policy applicable to the system or become the central provisions of a stand-alone policy that covers protection of privacy, civil rights, and civil liberties.
- The sections in Part C could be included in an interagency agreement among all the participating agencies that form or join an information sharing network or would be an addendum or separate agreement signed by the participating agencies.

It is important to note that the policy template sections proposed are NOT intended to be used "as is" without modification. The objective of the templates is to provide suggested language for use in drafting a policy or an interagency agreement. In some sections, alternative language may be provided or alternatives or additions may be suggested in the commentary. One purpose of suggested alternative language is to raise issues that may be relevant in one jurisdiction but not another or that may be relevant for one type of justice information system but not another.

Steps for Editing the Template Language

One stage of the process[9] of drafting a policy or agreement involves an agency using the templates contained in this document to build a policy. An agency should take the following steps to adapt the language provided in the templates to its justice information system:

1. Clarify the type of justice information system that will be covered by the policy—is it for an RMS, CMS, CJIS, IJIS, JMS, criminal intelligence system, or a combination? The nature of the system will determine the applicable language in key elements (for example, the data collection threshold or the access and disclosure rules).
2. Determine what policy parts are needed based on existing laws and organizational structures. Is the enabling authority of Part A needed? Will the operating policy covered in Part B be a stand-alone policy or be included in an existing policy? Are multiple agencies involved, suggesting the need for the interagency agreement proposed in Part C?

[9] For a more complete review of the privacy policy development process, see Global's *Privacy and Civil Liberties Policy Development Guide and Implementation Templates*, located at http://it.ojp.gov/documents/Privacy_Guide_Final.pdf.

3. Based on these decisions, the agency(ies) should review and edit each section proposed for the Part(s) identified as needed in the previous step and:
   a) Modify the language of relevant sections to include the language of or reference to statutes, rules, standards, or policies applicable to the agency on the subject of each section. Usually, the places where editing is needed are indicated [in italics in brackets]. However, sometimes the general rule stated in the proposed section will also need to be edited to comport with the law in the jurisdiction. A decision must also be made about including suggestions for additional language that are in italics and [brackets] or in the Commentary. In some cases, there may be gaps where no applicable law exists and the agency will have to determine what policy it will follow. Note that it would be helpful to address these policy gaps at a state level in a way that assists local jurisdictions (particularly smaller jurisdictions) in developing more complete policies.
   b) Delete sections i) that are not relevant, based on the information collection and sharing laws applicable in the agency's jurisdiction, ii) that are not relevant to the type of information sharing system for which the policy is being drafted, or iii) that the agency chooses not to include.
   c) Add sections for provisions that are not addressed in the templates but are required by the jurisdiction's information collection and sharing laws.
   d) Change key terms to those applicable to the agency's jurisdiction, especially those that have specific legal meanings. For example, the official title of the agency should be inserted in the definition of "agency" in Section B.3.10, and the name of the information system substituted where indicated. Other examples would be terms defined under Section B.3.00 or legal standards such as those in Subsection B.4.20 (b).
   e) Add details to lists identified in [brackets] in the sections, for example, a list of types of stored information about an individual that are not to be disclosed to that individual pursuant to Subsection B.7.50 (b) (4).
   f) Where indicated, include contact data for the office or person able to answer questions or provide additional information.

During the development process, it is very useful for the drafting committee to keep a record (for example, in minutes) of discussions and options considered. This record can serve as valuable "legislative history" during subsequent interpretation of the policy. It also demonstrates the thoroughness of the drafting committee's considerations and documents any policy gaps addressed.

Once the editing has occurred and necessary additions and changes are made, the draft policy should be submitted to the oversight body. That body should tentatively adopt the draft and circulate it among stakeholders for comment. After comments are received, the draft should be modified based on the comments received and then adopted by the oversight body. For further discussion of the overall policy development process, see Global's *Privacy and Civil Liberties Policy Development Guide and Implementation Templates*.[10]

[10] Located at http://it.ojp.gov/documents/Privacy_Guide_Final.pdf.

A. Elements of Enabling Legislation or Authorization

The following provisions should be included in the instrument or document that authorizes the creation of and designates the oversight body for the justice information system. The instrument could be an enabling statute, resolution, ordinance, or executive order at the local, state, tribal, territorial, or federal level. Not all justice information systems have an explicit enabling document. However, the authority to create the system may be found, at least in part, in budget authorizations or laws describing the conduct of the system that imply its existence. It is generally more effective to have an explicit enabling statement for transparency and accountability purposes, as well as to clarify the goals and limitations of the system. The statement should contain broad, general principles, not details. The details should be in the operational policy that includes the provisions suggested in Part B.

A.1.00 Statement of Purpose

The goal of establishing and maintaining the [*add the name of the justice information system and specify what type of system is involved, for example, a records management system, case management system, integrated justice information system, or criminal intelligence system*] is to further the following purposes:

(a) Increase public safety and improve national security;

(b) Minimize the threat and risk of injury to specific individuals;

(c) Minimize the threat and risk of injury to law enforcement and others responsible for public protection, safety, or health;

(d) Minimize the threat and risk of damage to real or personal property;

(e) Protect individual privacy, civil rights, civil liberties, and other protected interests;

(f) Protect the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information;

(g) Minimize reluctance of individuals or groups to use or cooperate with the justice system;

(h) Support the role of the justice system in society;

(i) Promote governmental legitimacy and accountability;

(j) Not unduly burden the ongoing business of the justice system; and

(k) Make the most effective use of public resources allocated to justice agencies.

Commentary

This section identifies 11 interrelated purposes underlying the development and operation of any type of justice information system. Although some do not appear to directly relate to the protection of privacy, civil rights, and civil

liberties, each contributes to the legitimacy of the system, thereby increasing a public sense of protection of these basic rights and interests.

These purposes will be achieved by a justice information system that provides complete, accurate, current, and timely information to justice system decision makers; improves the quality of justice system decisions; and increases the rate of apprehension and incarceration of offenders. Proper conduct on the part of individuals collecting information and who have access to information in the system furthers these purposes.

The purposes are not mutually exclusive, although some may be competing in some circumstances. They are not listed in priority order, although considerations of efficiency (Subsection (j)) and effective use of public resources (Subsection (k)) would not trump the interests in security, public and individual safety, and compliance with the law.

Subsection (a): Increase Public Safety and Improve National Security. The ultimate objective of a justice information system is to enhance public safety and improve the nation's security. This objective is accomplished by gathering and sharing information so as to increase the government's ability to detect, deter, defeat, and prosecute criminal, including terrorist, activities. This includes both reactive and proactive activities. Reactive activities include detecting, responding to, and investigating suspected criminal, including terrorist, activities and apprehending suspected criminals, prosecuting cases, and otherwise solving crimes. The expectation is that the prosecution of criminal acts will suppress future crimes, thereby improving public safety. Proactive activities include anticipating, identifying, deterring, preventing, and defeating potential criminal, including terrorist, activities. The expectation is that effective, integrated justice information systems will protect public safety and national security by preventing brutalities like the September 11, 2001, attacks or the Oklahoma City bombing.

Subsection (b): Minimize the Threat and Risk of Injury to Specific Individuals. Sometimes the gathering and sharing of information through a justice information system will identify a risk specific to an individual or group of people, as opposed to the public at large. Protecting individuals is a subset of public protection. Note that there are two aspects to this type of protection. One involves gathering and acting on information about a threat to a specific person, and the other involves protecting information in the justice information system about a specific person from disclosure that would endanger the person's safety. Personal safety can be enhanced by restricting access to information that could be used to injure someone physically, psychologically, or economically. Examples of potential injury to individuals based on information that could be in a justice information system include intimidation of or physical violence towards victims, witnesses, jurors, law enforcement, justice system personnel, or defendants, as well as repeated domestic violence or sexual assault, stalking, and identity theft.

Subsection (c): Minimize the Threat and Risk of Injury to Law Enforcement and Others Responsible for Public Protection, Safety, or Health. Another subset of public safety relates to the risk to law enforcement personnel and other public safety and protection personnel. Information gathered and kept in a justice information system can be used to identify threats and prevent injury to those responding to criminal incidents, natural disasters, or health emergencies of any type.

Subsection (d): Minimize the Threat and Risk of Damage to Real or Personal Property. Criminal, including terrorist, activities can also threaten or damage property. Gathering, analyzing, and sharing information can therefore also protect property or minimize loss to property resulting from criminal, including terrorist, activity. There is an additional aspect to this—protection of critical infrastructure. Justice system information can detect and reduce threats to public safety, public health, and our way of life resulting from the crippling or destruction of infrastructure such as power and water systems and transportation corridors or from the use of chemical and biological weapons.

Subsection (e): Protect Individual Privacy, Civil Rights, Civil Liberties, and Other Protected Interests. There are two aspects to this purpose. One relates to the role of government and the other to how government agencies conduct

themselves. One role of the government is to protect individuals' privacy, civil rights, and civil liberties; this is one aspect of public safety. The interest in privacy is protected by preventing inappropriate disclosure of certain kinds of information. Civil rights are obligations imposed upon government to promote equality. The state has a role in ensuring that all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of race, religion, gender, or other irrelevant characteristics. Justice information systems can assist agencies in this affirmative duty to protect individuals. The second aspect requires agencies to go about their work in a lawful manner. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference in the conduct of their lives.

Protecting and respecting privacy, civil rights and civil liberties also contributes to public trust and confidence that the justice system understands its role and promotes the rule of law.

Finally, it is important to remember that not everyone cataloged in a justice information system is a criminal. As part of protecting public safety, the justice system will collect and maintain information about victims, witnesses, and those who provide information to or come to the attention of the justice system. Erroneous information may have also been collected about someone, as when the wrong identity is given or assumed about someone being investigated, arrested, or otherwise associated with suspected criminal activity. Care should be taken that the privacy rights and interests of such third persons are not compromised by inappropriate collecting, storage, and disclosure of information in the justice information system.

Subsection (f): Protect the Integrity of the Criminal Investigatory, Criminal Intelligence, and Justice System Processes and Information. Creating and maintaining a justice information system should support justice processes, not undermine them. The activities associated with a justice information system and the collection, storage, analysis, and sharing of information should contribute to the integrity of the result. This will occur if the operations are conducted in a lawful manner and the outcomes are—and appear to be—just. The integrity of the system is enhanced when the information collected is relevant to the role of the system and is of high quality and when disclosure is properly managed so as not to compromise ongoing investigations or monitoring of activities.

Subsection (g): Minimize Reluctance of Individuals or Groups to Use or Cooperate With the Justice System. Individuals and groups will use and cooperate with justice system agencies if they perceive them to be lawful and effective. People will be reluctant to use or support the justice system if they perceive that the information gathered is irrelevant, that public officials are operating "outside the law," or that the information is gathered in a manner that puts people at risk of harm or disrespects their rights or privacy interests. There may also be an unintended effect of encouraging use of alternative solutions, whether in the form of self-help or extra-judicial actions. Conversely, people will have confidence in and will support a justice system that protects them and does so in a manner that respects the law.

Subsection (h): Support the Role of the Justice System in Society. The role of the justice system is to protect the public and prevent crimes, including terrorism. A justice information system should support this role by increasing the effectiveness and efficiency of the justice system in achieving a just result.

Subsection (i): Promote Governmental Legitimacy and Accountability. The operation of the justice information system must enhance accountability and promote legitimacy. In order for people to assess accountability, they must be aware of the existence of the justice information system and be able to evaluate the efficacy of its operations. This requires both openness and accountability regarding the operation of the justice information system. Violations of the operating policies of the system must be identified and appropriate sanctions enforced. Having operational policies available to the public, monitoring performance and compliance, and enforcing the policies promote accountability. A justice information system that integrates privacy and security protections and can document activity can be held accountable. These capabilities also promote greater public trust and confidence in the justice system, giving it greater legitimacy.

Subsection (j): Not Unduly Burden the Ongoing Business of the Justice System. The policies and operation of a justice information system should not unduly burden the justice system in fulfilling its fundamental role of protecting the public and individuals. Keeping too much or irrelevant information will not only be unhelpful, it may even impede work. Unnecessary or improper disclosure of information may also impede operations or diminish the integrity of investigations.

Subsection (k): Make the Most Effective Use of Public Resources Allocated to Justice Agencies. Sharing information leverages those public resources allocated to law enforcement and national security in several ways. Maintaining accurate, complete, and timely information in a justice information system reduces the waste of public resources from chasing false leads, duplicate information collection and entry, and erroneous linking of information from several sources. A robust information sharing system will also allow the larger justice system to "connect the dots" in ways that have not previously been possible.

A.2.00 Compliance With Laws Regarding Privacy, Civil Rights, and Civil Liberties

(a) The [*add the name of the justice information system governing body*] and all participating agencies, employees, and users will comply with all applicable laws protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing, and disclosure of information.

(b) The [*add the name of the justice information system governing body*] will adopt internal operating policies requiring compliance with all applicable laws protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing, and disclosure of information in the system.

Commentary

These provisions provide an explicit commitment by the agency and key participants to comply with all laws protecting privacy rights, civil rights, and civil liberties of individuals and organizations about whom the agency or users may collect and share information. The term "applicable" is included to confirm that the laws to be followed are those that apply to the agency and its personnel; there is no intent to subject the agency and its personnel to laws that would not otherwise cover the agency.

Subsection (b) requires the agency to adopt operational policies governing the information sharing system and its operations protecting privacy, civil rights, and civil liberties. Since this provision is intended to be in the enabling legislation, it is stated broadly. There may be a large body of law, whether legislative or judicial in origin, that specifies in detail what this provision means. That should not be listed here; rather, the requirements should be incorporated into the provisions in Part B.

A.3.00 Agency Transparency and Accountability

(a) The existence of the [*add the name of the justice information system*] will be made public and the systems policies on protection of privacy, civil rights, and civil liberties will be made available to the public on request and through any public Web site providing information about the system.

(b) The [*add the name of the justice information system governing body*] will adopt provisions to ensure accountability for compliance with all applicable laws and policies in the collection, use, analysis, retention, destruction, sharing, and disclosure of information.

Commentary

Making the existence of the justice information system public contributes to the credibility and legitimacy of the agency and information system by demonstrating that the agency has nothing to hide and is amenable to appropriate public oversight. It thus promotes purposes (g), (h), and (i) of Section A.1.00. Operators of criminal intelligence systems may want to consider the extent to which the existence of the system is made known publicly, recognizing that public disclosure which occurs only when a problem is publicized often exacerbates public concerns.

Subsection (b) states that the agency will be accountable for the use of the system and in its operation. Applicable laws and policies include local, state, tribal, territorial, or federal statutes, regulations, rules, court decisions, and policies.

B. Elements of a Basic Internal Operations Policy

The objective of an operations policy protecting privacy, civil rights, and civil liberties is to provide justice agency personnel, contractors, and users with guidelines and principles regarding the collection, analysis, use, retention, destruction, sharing, and disclosure of information kept in any type of justice information system. The provisions suggested in this part are intended to be incorporated into the general operating policies applicable to the justice information system or can form the substantive core of a stand-alone policy covering privacy, civil rights, and civil liberties. These provisions are intended to provide explicit and detailed guidance to agency personnel and other users about what the applicable laws offer or require for each of the topics covered.

Following the statement of purpose and definition sections, the policy elements are arranged in the order in which information is generally handled in a system. The template begins with the collection of information and then addresses analysis, use, dissemination and access, and retention. In addition, there are provisions related to the administration of the system, including agency accountability, policy enforcement, and the training of personnel.

B.1.00 Statement of Purpose

The goal of establishing and maintaining the [*add the name of the justice information system and specify what type of system is involved, for example, a records management system, case management system, integrated justice information system, or criminal intelligence system*] is to further the following purposes:

(a) Increase public safety and improve national security;

(b) Minimize the threat and risk of injury to specific individuals;

(c) Minimize the threat and risk of injury to law enforcement and others responsible for public protection, safety, or health;

(d) Minimize the threat and risk of damage to real or personal property;

(e) Protect individual privacy, civil rights, civil liberties, and other protected interests;

(f) Protect the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information;

(g) Minimize reluctance of individuals or groups to use or cooperate with the justice system;

(h) Support the role of the justice system in society;

(i) Promote governmental legitimacy and accountability;

(j) Not unduly burden the ongoing business of the justice system; and

(k) Make the most effective use of public resources allocated to justice agencies.

Commentary

See Commentary under Section A.1.00 in Part A.

B.2.00 Compliance With Laws Regarding Privacy, Civil Rights, and Civil Liberties

All participating agency personnel, personnel providing information technology services to the agency, private contractors, and users will comply with all applicable laws protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing, and disclosure of information.

Commentary

See Commentary under Section A.2.00 in Part A.

B.3.00 Definitions

The sections in this subpart provide definitions for words or phrases regularly used in this policy to explain their meaning in the context of this policy. An agency may want to (or need to) define other terms. References to definitions of other terms used in local, state, or federal laws or policies are provided in Appendix Five. While these definitions are stated only in Part B, it may be appropriate to include these definitions in documents containing language from Part A and Part C.

B.3.10 Definition of Agency

***Agency* refers to [*state the official title of the agency or agencies to which this policy applies*].**

B.3.20 Definition of Information

***Information* includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists.**

Commentary

Information is defined because the handling of information is the essence of the policy. The definition is very inclusive, because the policy is intended to apply to all types and manner of information sought and retained by an agency, not just information specific to an individual, often referred to as personally identifiable information. Civil rights laws and the integrity of the justice information system implicate the processes and practices of seeking and retaining information as much as the retaining and disclosure of information about a specific individual.

Information can exist in many different mediums and may simultaneously exist in more than one medium. The medium can be physical, hard-copy, or an electronic form. It includes documents, writings, electronic representations of text or graphic documents, and electronic images (including a video image) of a document, evidence, an object, or an event. It also includes information in the fields or files of an electronic database, an audio or video recording (analog or digital) of an event, or notes in an electronic file from which a transcript of an event can be prepared.

B.3.30 Definition of Law

As used in this policy, *law* includes any local, state, tribal, territorial, or federal statute, ordinance, regulation, executive order, policy, or court rule, decision, or order, as construed by appropriate local, state, tribal, territorial, or federal officials or agencies.

Commentary

In the interest of generating a comprehensive privacy, civil liberties, and civil rights policy, the definition is very broad, including items that may not be considered laws in a particular jurisdiction. It includes not only statutes or laws adopted by legislative bodies but also regulations and orders issued by an executive branch agency and decisions, rules, and orders of the judicial branch. The definition could also refer to policies adopted by any of the three branches, if any such policies exist and are relevant to the justice information system. Finally, it includes judicial interpretations, through case decisions, of the meaning or application of statutes and regulations.

B.3.40 Definition of Public

***Public* includes:**

(a) Any person and any for-profit or nonprofit entity, organization, or association;

(b) Any governmental entity for which there is no existing specific law authorizing access to the agency's information;

(c) Media organizations; and

(d) Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the agency.

***Public* does not include:**

(e) Employees of the agency;

(f) People or entities, private or governmental, who assist the agency in the operation of the justice information system; and

(g) Public agencies whose authority to access information gathered and retained by the agency is specified in law.

(h) [*Consider adding, if bulk release of information is permitted (see Subsection B.7.40 (e)): Public or private entities of any type, whether for-profit or nonprofit, that are authorized by law and obtain requisite permission to receive information in bulk from the agency.*]

Commentary

This definition is included for use in applying the sections providing for access to information by the public (see Section B.7.40).

Subsection (b) states that if there are no explicit provisions applicable to a governmental entity authorizing access and use of the information in the system, the employees of the agency will be treated as members of the general public for purposes of this policy.

Subsection (d) refers to entities that acquire information from many sources and compile them into a database to which their clients direct queries. Examples include credit bureaus, background screening entities, and other commercial database services.

Subsections (e) to (g) describe entities or individuals not defined as public.

Subsection (e) distinguishes agency employees from the public, as employees' access would be covered by Section B.7.10.

Subsection (f) includes other governmental entities, as well as private contractors, who provide services to the agency for the operation of the information system.

Subsection (g) addresses those situations where there is existing law or another policy that governs access to information by the employees of a particular public agency.

Subsection (h) is proposed for those jurisdictions that are authorized by law to release in bulk, to public or private entities, information in the system, including personally identifiable information for matching purposes. See proposed Subsection B.7.40 (e) regarding authority to release information in bulk.

B.4.00 Seeking and Retaining Information

The sections suggested in this subpart relate to the gathering of information and its retention by the agency. The provisions address 1) what information the agency is authorized to seek and retain, 2) what it is prohibited from seeking or retaining, and 3) what methods are permitted for seeking information. Issues associated with receiving information from third parties, including unsolicited information such as tips, are also addressed. Finally, there are provisions about categorizing information with respect to its validity, reliability, and access or disclosure.

B.4.10 What Information May Be Sought or Retained?

(a) This agency will seek or retain only information:

(1) [*for a records management system, case management system, jail management system, or other type of justice information systems, state the standard governing what information may be sought or received and retained in the system, for example:*] 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 that is useful in crime analysis or in the administration of criminal justice.

(2) [*for a criminal history record system*] Collected by criminal justice agencies on specific individuals, consisting of official identifiable descriptions and notations of arrests, detentions, warrants, complaints, indictments, information, or other formal criminal charges and any disposition relating to these charges, including acquittal, sentencing, pre- or postconviction supervision, correctional supervision, and release, but not [*include any exceptions describing information that will not be kept in the system, for example, fingerprint records where such information does not indicate the individual's involvement with the criminal justice system*].

(3) [*for a criminal intelligence system*] Where there is reasonable suspicion that a specific individual or organization has committed a criminal offense or is involved in or is planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and the information is relevant to the criminal (including terrorist) conduct or activity.

(b) This agency will not seek or retain information about an individual or organization solely on the basis of religious, political, or social views or activities; participation in a particular organization or event; or race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation.

(c) This agency will not seek or retain information about the political, religious, or social views; participation in a particular organization or event; or activities of any individual or his or her race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation unless such information is:

(1) Relevant to whether an individual or organization has engaged in, is engaging in, or is planning a criminal (including terrorist) activity; or

(2) Needed by the agency:

i) To identify an individual,

ii) In order for the agency to operate effectively, or

iii) To provide services to the individual or accommodate an individual's religious, ethnic, or cultural requests or obligations.

(d) The agency shall keep a record of the source of all information retained by the agency.

Commentary

This section addresses the content of information as opposed to the means by which the information is acquired (see Section B.4.20). The intent of this section is to explicitly state the rules the agency will follow regarding what information it may or may not seek or retain. It addresses:

- *What information the agency is authorized to seek and retain;*
- *Limitations on what information can be sought and retained; and*
- *What information the agency is prohibited from seeking and retaining.*

Note that the section refers to information sought or retained by the agency. The template language here applies to information contained in a justice information system, that is, information in electronic form. However, the standards stated in the section could apply equally to information in paper form.

The language of this section uses the phrase "seek or retain"[11] because the focus is on the actions of the agency, not of others. Laws that authorize or limit the actions of the government apply when the agency takes action, not when it passively receives information (addressed in Subsection B.4.20 (b)). However, such information, even if unsolicited, cannot be kept unless the appropriate legal standard is met for retaining information.

Subsection (a) states the standard for seeking and retaining information for the type of justice information system covered by the policy. An agency may have different standards for different types of information. If the policy will apply to more than one type of system, this section should include subsections stating the standard for each type of system.

Subsection (a) (1) states a standard for basic RMS, CAD, CMS, JMS, CJIS, or IJIS systems. The language is general and fairly broad in scope.

Subsection (a) (2) states a standard for criminal history record systems. It is based on, but not exactly the same as, the definition in the National Crime Prevention and Privacy Compact, 42 U.S.C. § 14616, repeated in 28 CFR Part 20, Section 20.3(d). Language suggested here that is not in the CFR section is indicated in italics.

Subsection (a) (3) states a standard for criminal intelligence systems. The language is derived from, but not identical to, 28 CFR Part 23, Section 23.20(a). Language suggested here that is not in the CFR section is indicated in italics. Note that the language an agency adopts must comply with 28 CFR Part 23, if applicable.

[11] Federal regulations for criminal history records systems use the terms "collecting, storing and disseminating" (28 CFR 20.20(a)), and the regulations for criminal intelligence systems use the terms "collect and maintain" (28 CFR 23.20(a)).

Because it also covers the retention of information, the standard in Subsection (a) should also be augmented to address what can be done with information that is received by the agency but was not actively sought. There is often a basis to seek or receive additional information when reasonable suspicion or probable cause has not yet been established (for example, to follow up on an anonymous tip). The standard needs to address the temporary retention and subsequent disposition of information that is received by the agency, along with any further information sought or received by the agency during the review of the unsolicited information but that is subsequently determined not to meet the agency standard for retention. Such information should be kept only long enough to determine whether it can appropriately be retained, and if not, it should be archived or destroyed in accordance with the applicable law or agency policy.

Subsection (b) states that the agency will not seek or receive any information about an individual or organization just because of the individual's or organization's political or religious views or because an individual participated in a particular association or event. Doing so would violate state, tribal, territorial, and federal laws about freedom of religion and association and equal protection. For example, information could not be collected and kept about individuals solely because they belonged to a particular church or had participated in a particular demonstration.

Subsection (c) prohibits an agency from collecting specific types of information about an individual or organization. The types of information that cannot be retained relate to protected activities, such as religion, political affiliation, and membership in an association. A list of local, state, tribal, territorial, and federal laws that might contain statements of information that cannot be collected is provided in Appendices One and Two.

Subsection (c) is not intended to prevent gathering and use of information that is relevant to justice purposes (Subsection (c) (1)) or the agency's operation (Subsection (c) (2)). For example, it does not prevent gathering of information about an organization or its members if the organization is engaged in criminal activity, even if the criminal activity is not the main purpose of the organization. Similarly, it would not prevent the gathering of such information if it is relevant to investigating or preventing criminal, including terrorist, activity—for example, information about witnesses, victims, family members, or associates concerning their credibility or that relates to an element of the crime (such as a hate crime). It also does not prevent an agency from collecting such information if it is needed by the agency to do its work, for example, noting an individual's race for identity purposes or a correctional facility collecting information on the religious practices of those in its custody.

Subsection (d) requires the agency to maintain information about the source of information that it keeps. Source information is relevant to categorizing information regarding its reliability and validity pursuant to Subsection B.4.30 (a). This is also necessary in order to assess, including during an audit, whether the collection of information has been in compliance with this policy and applicable laws. Note that the rules regarding access to and disclosure of source information may be different from the rule about the information provided by the source.

B.4.20 Methods of Seeking or Receiving Information

(a) Information gathering and investigative techniques used by this agency will comply with all applicable laws.

(b) This agency will not directly or indirectly receive, seek, accept, or retain information from an individual or nongovernment information provider, who may or may not receive a fee or benefit for providing the information, if the agency knows or has reason to believe that:

- **(1) The individual or information provider is legally prohibited from obtaining the specific information sought or disclosing it to the agency [*include any exceptions regarding illegally obtained information*];**
- **(2) The individual or information provider used methods for collecting the information that the agency itself could not legally use [*include any exceptions regarding illegally obtained information*];**

(3) The specific information sought from the individual or information provider could not legally be collected by the agency; or

(4) The agency has not taken the steps necessary to be authorized to collect the information.

(c) Information gathering and investigative techniques used by this agency will be no more intrusive or broadscale than is necessary in the particular circumstance to gather information it is authorized to seek or retain pursuant to Section [*B.4.10*].

Commentary

This section addresses the means of seeking and receiving information as opposed to its content (see Section B.4.10). It expressly states that information gathering will be done in a manner consistent with applicable laws. The limitations relate to both the method or technique of collection (Subsections (a) and (b)) and the breadth of the inquiry or search (Subsection (c)).

Subsection (a) states the general principle that information gathering techniques and methods will comply with applicable law. Federal laws that guide or limit information collection techniques by governmental agencies are identified in Appendix One. There may also be local, state, tribal, or territorial laws that guide or limit information collection techniques by governmental agencies. Lists of possible state laws, topics, and activities that may be covered by state laws are provided in Appendix Two.

By implication, this section also requires the agency to delete information that is subsequently found to have been obtained unlawfully (see Subsection B.5.00 (c) regarding deleting information).

Subsection (b) addresses information from nongovernmental sources, both individuals and third parties. This would include unsolicited information as well as that actively sought by the agency. Unsolicited information would include information received anonymously. Actively sought information would include that from organizations which maintain and make available information about individuals or organizations such as credit agencies or other information brokers. It would also apply to information obtained through the Internet using a search engine. The intent of the subsection is to prevent an agency or its personnel from circumventing the law applicable to it by using an individual or a nongovernmental, third-party source to obtain information.

Subsection (b) states a general requirement that information sought or received from an individual or nongovernmental source must have been obtained legally by the source and in a manner consistent with the agency's information gathering authority and limitations. No detailed legal standard or procedure is specified as to how it is to be established that the information was obtained appropriately and legally by the third party beyond the reference in Subsection (b) to "knows or has reason to believe." In a situation where the information is of a nature or type that the agency itself could not lawfully obtain directly, the agency personnel receiving the information should ascertain whether the information was obtained legally by the third party and whether it is legal for the third party to provide the information to the agency. Sometimes, it may not be apparent how the information was obtained or whether it was obtained legally. Finally, Subsection (b) makes it clear that whether or not the third party received a fee or other benefit for the information is not relevant to whether the agency can seek and retain the information.

Subsection (b) (1) provides that the agency cannot use information from this source if it is unlawful for the individual or information provider to obtain the information or to share the information with the agency.

Subsection (b) (2) precludes an agency from obtaining information from third parties who used information gathering methods that the agency itself could not use. Unfortunately, the application of this concept is not as simple as it might appear. For example, what is to be done with an anonymous tip? In this type of situation, the agency can certainly use

the information as a basis to investigate further, but the information should not be retained in the justice information system without having met the necessary standard or predicate specified in Subsection B.4.10 (a). A more problematic example involves criminal informants or cooperating defendants who often offer information that was not legally obtained but can be used by law enforcement as long as law enforcement did not direct them to illegally obtain the information. An agency may want to include some sort of exception in this section that states the agency's policy regarding such circumstances.

Subsection (b) (3) prevents an agency from getting information from a third party if it could not get the information itself. The section does not prevent an agency from getting information from a third-party source who has aggregated information from many sources, as long as the source obtained the information lawfully and the agency could lawfully gather the specific pieces of information sought. While the agency itself might not be able to lawfully aggregate information on people or organizations the way an information provider can, if the agency itself could have gathered the specific information about an individual or organization, it can get the information from the provider under this subsection. Note that the agency should not ask or encourage information to be aggregated if the agency could not collect and aggregate the information itself.

Subsection (b) (4) requires the agency to comply with applicable procedures for obtaining authority to collect information. For example, if a search warrant is required to gather certain information, this provision requires the agency to obtain a proper warrant, even if the information will be provided by a third party.

Subsection (c) states the principle that information gathering will only be as broad as necessary to gather relevant information. Overly broad or intrusive methods are discouraged. Overbroad gathering increases the risk of invading privacy and infringing civil rights and civil liberties, as well as wasting limited agency resources, discouraging cooperation, and undermining the legitimacy of the agency. There may be existing laws or policies regarding specific information gathering techniques, such as for wiretapping, that should be referenced here.

One aspect of seeking and receiving information that is implicated by this subsection is the scope of aggregation of information about people or organizations in a justice information system. A typical system covered by this template represents an aggregation of information about people, organizations, events, property, etc. The collected information may or may not have been readily searchable before being put in electronic form. Once in electronic form, the ability to rapidly search and analyze the information increases the concern about whether the aggregation is legal, reasonable, and cost-effective. The agency should evaluate the scope of the information sought and retained in the aggregate and the accumulation in the entire justice information system, as well as at each stage of gathering each item of information.

B.4.30 Classification of Information Regarding Validity and Reliability

(a) At the time of retention in the system, the information will be categorized regarding its:

- **(1) Content validity;**
- **(2) Nature of the source; and**
- **(3) Source reliability.**

(b) The categorization of retained information will be reevaluated when new information is gathered that has an impact on the validity and reliability of retained information.

Commentary

The objective of categorization is to let subsequent users assess the extent to which they can rely on the information. The expectation is that when the information is first retained, it will be coded as to its content validity and source reliability. The section applies to law enforcement, criminal intelligence systems, and other systems in which the person reviewing the information needs to know about its validity and reliability. It does not apply to systems, such as a court case management system, in which validity and reliability are addressed more openly, for example, in a court hearing.

Subsection (a) (1), content validity, has to do with the accuracy or truth of the information itself, as opposed to its source.

Subsection (a) (2), nature of the source, provides an indication of the type or nature of the origin of information. Examples of categories characterizing the source of the information could include 1) an anonymous tip, 2) an informant, 3) law enforcement interviews of individuals—in particular a victim or witness, 4) a public records source, 5) a nongovernmental information provider, etc.

Subsection (a) (3), source reliability, addresses the consistency of the content validity of information obtained from a particular source over time.

Subsection (b) requires updating of the categorization of information when new information clarifies the validity or reliability of previously retained information. This is a significant requirement that may be difficult to maintain when the amount of information in the system is extensive, which may be the case in a typical justice information system, particularly after it has been in use for a period of time. Updating the validity, source, or reliability coding may then only occur as users analyze information in light of new information, but not every time information is added to the system. There is also an issue if the volume of information being added is such that users do not take the time to properly code the information at the time of initial entry because it is too time-consuming. Entering and updating reliability and validity codes is more important in a criminal intelligence system where there is a higher standard regarding when information can be kept.

B.4.40 Classification of Information Regarding Limitations on Access and Disclosure

(a) At the time a decision is made to retain information, it will be classified pursuant to the applicable limitations on access and sensitivity of disclosure in order to:

- **(1) Protect confidential sources and police undercover techniques and methods;**
- **(2) Not interfere with or compromise pending criminal investigations;**
- **(3) Protect an individual's right of privacy and civil rights; and**
- **(4) Provide legally required protection based on the status of an individual as [*indicate classes of individuals accorded protection regarding access to or disclosure of sensitive information, for example, as a victim of crime or domestic violence or as a witness*].**

(b) The classification of existing information will be reevaluated whenever:

- **(1) New information is added that has an impact on access limitations or the sensitivity of disclosure of the information; or**
- **(2) There is a change in the use of the information affecting access or disclosure limitations.**

(c) The access classifications will be used to control:

- **(1) What information a class of users can have access to;**
- **(2) What information a class of users can add, change, delete, or print; and**
- **(3) To whom the information can be disclosed and under what circumstances.**

Commentary

This section requires an explicit classification of information as to the ability of any particular class of persons to access the information or of the agency to disclose the information. This is one of the primary mechanisms for implementing many of the purposes stated in Section B.1.00. The section requires the classification to "attach" to the information when a decision is made to retain the information in the justice information system. The classification could be a flag or field associated with the information, such as some form of XML tag.

Access categorization can be subject to abuse because it allows information to be hidden from view. It should not be used to limit access to information to 1) conceal errors or sloppiness in entering or categorizing information, 2) conceal incompetence or violations of law in seeking or retaining information (for example, for political purposes), 3) prevent embarrassment to a person or agency, or 4) limit access to information that is not required to be protected. An agency may want to add a subsection specifically prohibiting inappropriate or wrongful categorization (see Section B.9.30).

Subsection (b) indicates two circumstances in which the access category may change. The first circumstance occurs when other or newer information becomes known that changes the nature of permitted access. An example would be an instance in which the identity of an alleged criminal becomes known, or new information suggests the imminence of criminal, including terrorist, activity. The second circumstance occurs when the subsequent use of the information results in different rules becoming applicable. An example of this occurs when information that is otherwise nonpublic is introduced into a court case and, by virtue of being in the court file, becomes a public record. The character of information may change again, including returning to a more private state (for example, when a conviction is expunged). The agency needs to determine what other boundaries exist where the transfer or exchange of information changes its categorization.

Subsection (c) states the uses of the classifications. The classification can be used to control both access (Subsection (c) (1)) and dissemination (Subsection (c) (3)). The classification is also relevant to who can add or modify information in the system (Subsection (c) (2)).

B.5.00 Information Quality

(a) The agency will make every reasonable effort to ensure that information sought or retained is:

- **(1) Derived from dependable and trustworthy sources of information;**
- **(2) Accurate;**
- **(3) Current;**
- **(4) Complete, including the relevant context in which it was sought or received and other related information; and**
- **(5) Merged with other information about the same individual or organization only when the applicable standard [*in Section B.6.20*] has been met.**

[or]

(a) The agency will comply with [*cite the applicable state law or policy setting forth information quality standards comparable to those specified above*].

(b) The agency will make every reasonable effort to ensure that only authorized users are allowed to add, change, or delete information in the system.

(c) The agency will make every reasonable effort to ensure that information will be deleted from the system when the agency learns that:

- **(1) The information is erroneous, misleading, obsolete, or otherwise unreliable;**

(2) The source of the information did not have authority to gather the information or to provide the information to the agency; or

(3) The source of the information used prohibited means to gather the information [*note any exceptions; see Subsection B.4.20 (b) (2)*].

(d) The agency will advise recipient agencies when information previously provided to them is deleted or changed pursuant to Subsection (c) when [*specify the circumstances in which notice of change or deletion will be made, for example, when the requesting agency has specifically requested to be notified or for particular types of changes or deletions, the information has been sealed or deleted*].

Commentary

This section lists the attributes of information quality that are required for information to be sought or retained by the agency. The requirement here is that agency personnel not seek unreliable information and not keep information once it has been found to be unreliable. These quality attributes are not required of information that is unsolicited and information that has not yet been evaluated for its quality (that is, when it is first acquired), although the section does apply if the decision is made to keep the information.

The first three subsections of (a) list the commonly understood aspects of information quality—it should be accurate, current, and from a reliable source. "Accuracy" encompasses the truthfulness of the information itself, any coding of the information, correct data entry when the information is added to the justice information system, and the data structures of the justice information system itself. There are several tools and business practices available to improve accuracy. They include such things as edit checks during data entry, the use of table-driven database structures, and referencing external data validity systems, for example, the U.S. Postal Service Address Verification service. Another way to improve accuracy is to allow individuals to see the information about themselves and seek to correct inaccuracies they perceive. However, this is often inadvisable for justice system information because of risks to individual and public safety. This is discussed in more detail in Section B.7.50, particularly Subsection (c).

Subsection (a) (3) refers to the "currency" of the information. Information that is old or stale may no longer have the relevant context and may be misleading or distracting. This is also a concern regarding information obtained from third-party sources, governmental or otherwise (see Subsection B.4.20 (b)).

Subsection (a) (4) addresses the "completeness" of the information. For information to be most useful to law enforcement, criminal intelligence, and justice communities—as well as others responsible for public protection, safety, or health—the full context must be collected and retained. This includes the context in which the information was obtained as well as seeking and retaining the whole story.

Under Subsection (a) (4), information that may be exculpatory should also be gathered and retained. For example, for arrest information, the system should include the disposition of the arrest when it occurs. A specific problem relates to a person's use of someone else's identity when arrested to avoid being discovered as someone with a criminal history or having outstanding warrants or other holds. When the correct identity is established, the arrest record for the person whose identity was misused should be augmented to indicate the misuse and make clear that the person does not have an arrest record.

Subsection (a) (5) refers to the merging of information from more than one source. See Subsection B.6.20 (b) for language on the standard for merging information.

The alternative Subsection (a) is for use when there is an existing law or policy defining information quality, which this policy should refer to rather than restate.

Subsection (b) refers to "authorized users." The implication is that the agency has established processes whereby users are not given authorization to add, change, or delete information until they have been trained and are considered qualified and competent to use the system.

Subsection (c) establishes an affirmative obligation to delete information that no longer has the requisite information quality. It identifies the typical reasons for deleting information. The reasons include factors related to the collection of the information as well as its inherent quality.

Subsection (d) addresses what should be done regarding information that has been shared with others. It requires the agency to inform other agencies about changes or deletions to information under certain circumstances. Requiring notice to every requestor whenever there is a change or deletion may be an onerous requirement, particularly if there has been significant sharing of information on a daily basis. The bracketed language would indicate when notice would be provided, based upon the nature of the inquiry or significance of the information.

Subsection (d) does not specify how the notice of change or deletion would be made. Options would include requiring a requestor who wanted notice to provide an e-mail address to which notice could be sent.

B.6.00 Collation and Analysis of Information

B.6.10 Collation and Analysis

(a) Information sought or received by the agency or from other sources will only be analyzed:

- **(1) By qualified individuals;**
- **(2) To 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 generally; and**
- **(3) To further crime (including terrorism) prevention, enforcement, force deployment, or prosecution objectives and priorities established by the agency.**

(b) Information sought or received by the agency or from other sources will not be analyzed or combined in a manner or for a purpose that violates Subsection [*B.4.10 (b)*].

Commentary

This section is primarily intended for criminal intelligence systems but may be relevant to records management systems or other types of justice information systems.

Subsection (a) (1) requires that the collation and analysis of information be performed by qualified individuals. This is in recognition that knowledgeable and skilled individuals are more likely to conduct the analysis in a professional, efficient, effective, and legal manner.

Subsection (a) (2) incorporates a use-type restriction similar to the collection restrictions described in Section B.4.10.

Subsection (a) (3) is similar to the restriction on gathering and storing information, in that it requires that analysis of information only be done in furtherance of and consistent with the purposes set forth in Section B.1.00.

Subsection (b) reiterates the prohibitions acknowledged in Subsection B.4.10 (b) about not collecting or compiling information based on improper criteria, such as religious or political views.

Recent advances in analytical approaches using anonymized data can provide an alternative to the exchange and analysis of data sets containing personally identifiable information on individuals. Using this technique, the personal identifiers in a set of data are replaced with new, anonymous identifiers before any analysis is done. After the analysis is done and if criminal, including terrorist, activity is detected, the analysts can request from the agency holding the source information the release of the actual personal identifiers for individuals of interest identified through the analysis. Such a process reduces the risk and stigma of investigation with an ulterior motive and the improper use or disclosure of information about specific individuals.

B.6.20 Merging of Information From Different Sources

(a) Information about an individual or organization from two or more sources will not be merged unless there is sufficient identifying information to reasonably conclude that the information is about the same individual or organization.

(b) The set of identifying information sufficient to allow merging will consist of [*specify a standard or set of information or characteristics that are considered adequate to allow merging of information*].

**[*Consider adding the following subsection to allow tentative matching of information from more than one source:*
(c) If the matching requirements are not fully met but there is a strong partial match, the information may be associated if accompanied by a clear statement that it has not been adequately established that the information relates to the same individual or organization.]**

Commentary

This section addresses a concern that becomes of greater significance as more information is shared across agencies and with private sector partners and as more information is acquired from third-party sources. For purposes of this section, "merged" means that information from different sources is linked in the system as referring to the same individual or organization.

Justice system effectiveness is leveraged by the ability to combine information from different sources to develop a complete picture of activities and threats—to "connect the dots"—without duplicating efforts. Accurate merging has a number of benefits, including better identification of individuals, more complete information on persons of interest, fewer false leads, fewer false positives, less opportunity for fraud and abuse by suspects, and less risk of bad press or lawsuits from misidentification or erroneous merging. However, work will be hampered and resources wasted if information that does not relate to the same person or organization is erroneously combined as if it did. This section establishes the basis for a digital due diligence before merging information from separate sources.

A complicating aspect is that matching assumes the data sources both have the same meaning, structure, and coding for the factors upon which matching is to be done; for example, both use the same conventions regarding how to format and spell a person's name.

Subsection (b) requires the agency to specify a standard for merging information. The standard would specify which combination of characteristics would permit information from two or more sources to be linked as referring to the same person or organization. Examples of information, characteristics, or attributes that, in combination, could establish that information from two or more sources is, indeed, about the same individual include:

- *Full name;*
- *Date of birth;*
- *Fingerprints;*
- *Law enforcement or corrections system identification number, usually based on fingerprints;*

- *Photograph;*
- *Physical description: height, weight, eye color, hair color, race, ethnicity, tattoos, scars, etc.;*
- *Social security number;*
- *Driver's license number;*
- *Contact information, such as address, phone number, e-mail, etc.; and*
- *Other biometrics, such as DNA, retinal scan, facial recognition, etc.*

A more generic standard might state, "all available attributes that can contribute to higher accuracy of match."

In a noncriminal setting, one way to verify a match is to check with the person about whom the information is being matched (this is the approach of the Federal Computer Matching and Privacy Act). This is often not advisable and may not be possible in a criminal justice setting.

When considering information about organizations as opposed to individuals, the characteristics or attributes that, in combination, could establish that information from two or more sources is, indeed, about the same organization are more problematic. Possibilities include the organization's name, federal or state tax ID number, and contact information such as office address and telephone number.

Subsection (c) suggests an optional provision to address the circumstance in which it appears that information from different sources relates to the same person or organization, but the standard for merging has not been fully met. A common circumstance in which this is relevant is in gang monitoring. The optional provision requires it to be made clear that the standard has not been met even if the preliminary assessment is that the information appears to be about the same person or organization. Pending the collection of further information to meet the standard, there still may be a value in indicating the possibility of a match for those querying the information system (see Subsection B.4.30 (a)) or categorizing information regarding its validity and reliability.

There are several approaches for indicating the match is incomplete. A disclaimer could be included with the response to a query or with any report containing the information—the electronic equivalent of a red stamp on the file. There could also be a requirement for independent verification of the match by anyone querying and using the information. Another way to reduce negative consequences of hypothesizing such an association is to limit who can access the information.

B.7.00 Sharing and Disclosure of Information

The sections in this subpart address to whom and under what circumstances information in the justice information system may be disclosed. Disclosure may be passive, allowing access through queries to the justice information system, or active, disseminating or publishing the information, for example, in bulletins or notices.

The situations covered in this subpart are organized by the category of person or entity who is seeking access to information: law enforcement officer, specific-use provisions, the public, and the person about whom information is stored in the system. This is based on the assumption that access rules are often stated on the basis of the status of the requesting individual or entity with respect to the information and the system. Alternatively, the concepts in these sections could be organized according to the type of information sought (for example, arrest information, conviction information, or warrant information) or organized according to the relationship of a person about whom information has been retained and may be shared or disclosed (for example, information about a defendant, victim, or witness) to the justice system.

For some types of justice information systems, the access and disclosure rules may provide for very limited access and disclosure. For example, the information in criminal intelligence systems generally is not publicly available.

B.7.10 Sharing Information Within the Agency and With Other Justice System Partners

(a) Access to information retained by this agency will only be provided to persons within the agency 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 the law and procedures applicable to the agency for whom the person is working.

[*Consider adding, if the person who gathered information is allowed to have access to it even if they would not be allowed access if they had not gathered it, the following provision: The person who received, reviewed, or added information to the system may be authorized to view the information he or she provided regardless of the type of access associated with the information or the contributor's access authority.*]

(b) An audit trail will be kept of access by or dissemination of information to such persons.

Commentary

This section governs sharing within the agency and with associated government agency personnel. These are the primary users of the information—generally the information system was created to help them do their job more effectively and at less cost. The allowed uses are intended to include all phases of law enforcement, from crime investigation through prosecution and adjudication to carrying out and monitoring the sentence. This encompasses agencies and entities such as law enforcement, prosecution, defense counsel, courts, pretrial services, probation, parole, and corrections at the local, state, tribal, territorial, or federal level.

Subsection (a) specifies a number of requirements regarding access and use. It states that the agency will only share the information it retains with government personnel who 1) are allowed to have access to this type of information; 2) will use it for law enforcement, public protection, or justice purposes—that is, they have a right to know; and 3) will use it in the performance of their official duties—that is, they have a need to know. The intent is to make it clear that just because a person has access by virtue of where he or she works or his or her role, the information available cannot be used for personal or other non-law enforcement inquiries or for inquiries not related to that person's work.

Subsection (b) provides that a record be kept of all access, by whom, and to what information. While retaining such a record might have the effect of discouraging access, it is an effective means of discouraging unnecessary or improper access and of tracing improper access for enforcement purposes (see Section B.9.30).

B.7.20 Sharing Information With Those Responsible for Public Protection, Safety, or Public Health

(a) Information retained by this agency may be disseminated to individuals in public or private entities only for public protection, safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures.

[*Add for a criminal intelligence system: Nothing in this policy shall limit the dissemination, including unsolicited, of an assessment of criminal intelligence information to a government official or to any other individual, when necessary to avoid imminent danger or certain danger to life or property.*]

[*Consider adding: (b) The agency shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.*]

(b) An audit trail will be kept of the access by or dissemination of information to such persons.

Commentary

This second disclosure section governs access to information by people and agencies whose duties are to protect the public, ensure public safety, or protect the public health. These individuals and entities may be more successful in preventing or stopping criminal, including terrorist, activities if they have timely access to certain types of information about threats, activities, or individuals. There is a wide range of entities, governmental and private, that might be entitled to information under these circumstances. Public protection would include security forces at locations or events involving large numbers of people (for example, sporting events and amusement parks), at critical facilities such as water and power plants and transportation links, and at installations whose operations, if disrupted, pose a threat to the public, such as chemical plants. It could also include individuals involved with other critical public services, such as transportation, communication, or financial centers. Public safety and public health include such agencies as fire departments, emergency medical and public health departments, and even agencies involved with mental health problems.

This section does not allow unfettered access. Subsection (a) provides for access only to those who have both a "right to know" and a "need to know" information that allows them to better protect public health or safety.

The optional Subsection (b) addresses the question of confirming or denying the existence of information that itself is not subject to public access. The subsection provides that the existence of information will not be confirmed or denied to someone who is not entitled to the information whose existence is being questioned. This prohibition 1) protects any confidentiality or privacy interests in the information, 2) protects the integrity of the investigatory or justice-related processes, and 3) contributes to public confidence in the system.

Subsection (c) provides that a record be kept of access. While retaining such a record might have the effect of discouraging access, it is an effective means of both discouraging unnecessary or improper access and of tracing improper access for enforcement purposes. The access is authorized because of the policy interest in public safety. The threat this access entails to privacy is mitigated somewhat by the requirement in Subsection (c) to maintain a record of who accessed the information so that violations of privacy can be detected and prosecuted.

B.7.30 Sharing Information for Specific Purposes

(a) Information gathered and retained by this agency may be disseminated for specific purposes upon request by persons authorized by law to have such access and only for those uses or purposes specified in the law.

[*Consider adding: (b) The agency shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.*]

(c) An audit trail will be kept of the requests for access and of what information is disseminated to such persons.

Commentary

Certain individuals or entities, including nongovernmental entities, may be entitled by law to access information contained in justice systems that is not available to the general public. For example, government officials, public agencies, licensing boards, and certain nongovernmental agencies may be entitled to information about the criminal history of an individual applying for services, employment, or benefits. Other examples of organizations that may be entitled to access, at least for limited purposes and for only certain information, include:

- *Government officials not in law enforcement or the justice system who are responsible for making public safety decisions on behalf of the public regarding facilities or services;*
- *Government officials not in law enforcement or the justice system who are responsible for making public health decisions;*

- *Government officials not in law enforcement or the justice system who are responsible for making entitlement or allocation decisions for individuals to receive government services or benefits, for example, public housing, health care, or welfare;*
- *Critical infrastructure protection or security entities (public or private);*
- *Professional licensing boards;*
- *Employers (public or private) hiring individuals for specific duties, such as bus drivers, airport workers, child care workers, etc.;*
- *Domestic violence shelters;*
- *Businesses or organizations particularly susceptible to cybercrime and identity theft; and*
- *Individuals or organizations conducting research, evaluation, or statistical studies who are monitoring or reporting about the activities or performance of an agency or the clients served by the agency, with appropriate institutional review board oversight.*

Subsection (a) requires that the individual be authorized to have access and that the use must be for the purpose specified in the law permitting access.

The optional Subsection (b) addresses the question of confirming or denying the existence of information that itself is not subject to public access. The subsection provides that the existence of information will not be confirmed or denied to someone who is not entitled to the information whose existence is being questioned. One example of this is criminal convictions that have been expunged or sealed where there are public policy decisions that even the existence of the former conviction should not be revealed. This prohibition 1) protects any confidentiality or privacy interests in the information, 2) protects the integrity of the investigatory processes, and 3) contributes to public confidence in the system.

Subsection (c) provides that a record be kept of all access. While retaining such a record might have the effect of discouraging access, it is an effective means of both discouraging unnecessary or improper access and of tracing improper access for enforcement purposes. The access is authorized because of the policy interest in public safety. The threat this access entails to privacy is mitigated somewhat by the requirement in Subsection (c) to maintain a record of who accessed the information so that violations of privacy can be detected and prosecuted.

B.7.40 Disclosing Information to the Public

(a) Information gathered and retained by this agency [*may/will*] be disclosed to a member of the public only if the information is defined by law to be a public record and is not excepted from disclosure by law, and it may only be disclosed in accordance with the law and procedures applicable to this agency for this type of information.

[or]

(a) The agency will ensure that information gathered and retained by this agency [*may/will*] be disclosed to a member of the public only if the information complies with [*cite the applicable law or policy setting forth public access to information*].

(b) The agency shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.

(c) An audit trail will be kept of all requests and of what information is disclosed to a member of the public.

[*(d) Add provisions regarding the fees, if any, that will be charged to those requesting information.*]

[*(e) Add provisions regarding bulk or compiled distribution of information to third parties if the agency will allow such access. Also address charging a fee for information "sold" to third parties.*]

Commentary

This section governs public access—access by anyone who is not entitled to access pursuant to one of the prior sections. Subsection (a) indicates when information may be disclosed to the public (see definition of "public" in Section B.3.40). It permits disclosure to the public of information that is specifically designated as a public record. Examples of this include such things as court records and conviction information. The subsection also permits disclosure of information to the public when such access is specifically allowed by law for information that would otherwise not be public. Examples include such things as police blotters, sex offender registries, and information about fugitives who are subject to arrest. An alternative provision is suggested for which there is a relevant and applicable law covering public access, for example, a public records act or freedom of information act.

The subsection also provides that the information can only be disclosed in the manner permitted by the law authorizing public access. For example, the information cannot be disclosed selectively to some members of the public, but not others. Another example would be restrictions in some jurisdiction that arrest information can only be requested chronologically, not by name, to avoid the ability to build arrest histories retroactively one at a time.

Subsection (b) addresses the question of confirming or denying the existence of information that itself is not subject to public access. The subsection provides that the existence of information will not be confirmed or denied if the information whose existence is being questioned is not public information. This prohibition 1) protects any confidentiality or privacy interests regarding the information, 2) protects the integrity of the justice processes, and 3) contributes to public confidence in the system.

Subsection (c) provides that a record be kept of disclosure. The record is to indicate both to whom disclosure was made and what information was disclosed. While retaining such a record might have the effect of discouraging access, it is an effective means of both discouraging unnecessary or improper access and of tracing improper access for enforcement purposes. The access is authorized because of the policy interest in public safety and open government records. The threat this access entails to privacy is mitigated somewhat by the requirement in Subsection (c) to maintain a record of who accessed the information so that violations of privacy can be detected and prosecuted, as well as deterred.

Subsection (c) assumes that it is legal to keep records of public access requests. In some instances, this may not be permitted under local or state laws. There may also be limitations regarding access to information about the requestor collected as part of the logging process.

Subsection (d) is included as a placeholder for the agency to use if it will charge a fee for providing information from the system.

Subsection (e) is included as a placeholder for the agency to use if it decides that bulk or compiled disclosure of information from the system is permitted and appropriate. In many states, access to individual records may be allowed, but bulk access is not. In addition, there may be a distinction between information about individuals when the individual is identifiable and information that is more aggregate in nature, and one cannot identify a specific individual from the information provided. The subsection could also contain language about whether information can be "sold" to third parties and what the fee is.

B.7.50 Disclosing Information to the Individual About Whom Information Has Been Gathered

(a) Upon satisfactory verification of his or her identity and subject to the conditions specified in (b), an individual is entitled to know the existence of and to review the information about himself or herself that has been gathered and retained by the agency. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information. The agency'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.

(b) The existence, content, and source of the information will not be made available to an individual when:

- **(1) Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution;**
- **(2) Disclosure would endanger the health or safety of an individual, organization, or community;**
- **(3) The information is in a criminal intelligence system; or**
- **(4) The information relates to [*specify what types of information are not to be disclosed to an individual under the law applicable to the agency*].**

(c) If an individual has objections to the accuracy or completeness of the information retained about himself or herself, the agency will inform the individual of the procedure for requesting review of any objections. The individual will be given reasons if a request for correction is denied. The individual will also be informed of the procedure for appeal when the agency has declined to correct challenged information to the satisfaction of the individual about whom the information relates.

[*(d) Add provisions regarding the fees, if any, that will be charged to those requesting information; for example, the agency may charge a fee for disclosure that reflects the cost to the agency for locating and reproducing the information (specify any exceptions to charging a fee*).]

(e) A record will be kept of all requests and of what information is disclosed to an individual.

Commentary

Subsection (a) states that an individual is entitled to know of and review information about himself or herself that is retained by the agency. The individual must verify his or her identity before obtaining access. The only information to be disclosed is that specifically about the individual requesting disclosure.

Subsection (b) lists exceptions to disclosure of information about an individual. If disclosure would inhibit an active investigation, the information need not be disclosed. If disclosure would endanger someone (for example, a victim, witness, informant, or law enforcement personnel) or some organization, the information need not be disclosed. If the information is part of a criminal intelligence system, it need not be disclosed. Some agencies, for example, correctional institutions, may want to include further restrictions (in Subsection (b) (4)) to avoid such requests interfering with the operations of the institution (see Section B.1.00 (j)). Finally, there may be local or state laws further limiting disclosure of information to an individual, and they should be specified or referred to in this section.

Subsection (c) relates to the process by which an individual may seek review of information that the individual alleges to be incorrect or incomplete.

Subsection (d) is included as a placeholder for the agency to use if it will charge a fee for providing information from the system.

Subsection (e) provides that a record be kept of all disclosure requests. While retaining such a record might have the effect of discouraging access, it is an effective means of both discouraging unnecessary or improper access and of tracing improper access for enforcement purposes (see Section B.9.30).

Provision is made in proposed Subsection B.9.20 (h) for a situation in which information about an individual has been obtained by someone not authorized to have it and this ought to be brought to the attention of the individual so steps can be taken to protect from harm.

B.8.00 Information Retention and Destruction

The following sections on records retention are included because of their impact on the protection of privacy, civil rights, and civil liberties. Once information is deleted or returned according to applicable retention schedules, it is no longer at risk of being improperly accessed, shared, or disclosed. Information that is no longer kept in a justice information system cannot infringe on anyone's privacy rights or interests, civil rights, or civil liberties. If the agency already has a robust records retention policy, the language of Section B.8.20 can contain a reference to the applicable records retention policy.

B.8.10 Review of Information Regarding Retention

(a) Information will be reviewed for purging [*specify periodic basis, such as annually, or reference the applicable law*].

(b) When information has no further value or meets the criteria for removal under applicable law, it will be purged, destroyed, deleted, or returned to the submitting source.

Commentary

This section explicitly states the policy of requiring periodic review of information to determine whether it should be purged from the justice information system. The intent of this section is not only to ensure compliance with any applicable records retention policy (Subsection (a)) but also to encourage a review that may remove information that no longer has value before it would be required to be purged by applicable records retention policies (Subsection (b)). This reflects a proactive approach to managing justice system information.

B.8.20 Destruction of Information

(a) The agency will delete information or return it to the source according to the following schedule:

[*Reference the law(s) specifying the applicable record destruction standard or schedule*]

[or]

[*If there is no applicable law, specify the destruction standard or schedule applicable to the system's records*].

(b) Permission to destroy or return information or records will be obtained from:

[*Reference the law(s) specifying whose permission must be obtained before destroying information or records*]

[or]

[*If there is no applicable law(s), specify whose permission, if any, must be obtained before destroying information or records*].

(c) Notification of proposed destruction or return of records will be provided to:

[*Reference the law(s) specifying to whom notice must be provided about the proposed destruction of information or records*]

[or]

[*If there is no applicable law, specify who, if anybody, must be notified about the proposed destruction of information or records*].

[*Consider adding: (d) The time period for purging information concerning an individual may be tolled during the time that an individual is in prison serving a sentence.*]

(d) A record that information has been purged or returned shall be maintained by the agency.

Commentary

This section specifies when review and purging of information in a justice information system is to occur and what the business process should involve. The policy can either reference relevant existing laws or provide the specific language about retention periods, destruction schedules, permission, and notice adopted by the agency if there is no applicable law. An alternative to periodic manual review would be to develop software that automatically purges information at the end of a specified period or notifies someone of the intent to purge.

The section is silent about whether the information is purged only from the live system or also from backups, archived data, or other forms of offline media. Purging from offline media presents an additional set of logistics problems. However, there should be procedures in place that prevent backup media that contains information subsequently deleted from the live system from being reloaded if the live system crashes.

If information has been provided to third parties, in particular to members of the public, notifying them of the subsequent destruction of the information, as required in Subsection (c), can be problematic. If information has been provided in bulk or compiled form, it may be easier to achieve elimination of copies of the information. For example, the agreement allowing bulk requests can require the requestors to regularly update their information to purge information that the agency has destroyed. The most effective way to limit use of purged information is to provide some penalty, fiscal or penal, if someone uses such information without checking to make sure it is still current.

Subsection (d) proposes a provision to suspend the time for purging a record while a person is in prison. The objective is to have the information about a person's criminal activity not be purged because the person is serving a prison term that exceeds the general retention period for this type of information. There may be other circumstances in which the retention period should be extended that the agency should consider.

B.9.00 Accountability and Enforcement

B.9.10 Information System Transparency

(a) The policy establishing protections of privacy, civil rights, and civil liberties will be made available to the public on request and through any public Web sites providing information about the system.

(b) The agency will designate a person responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system and will provide to the public the [*position title*] contact information.

Commentary

Subsection (a) implies that the existence of the justice information system will be known to the public by requiring the privacy and civil liberties policy to be made available to the public. Acknowledging the existence of the system demonstrates the willingness of the agency to be subject to appropriate public scrutiny and contributes to public confidence in the agency and its operations.

Subsection (b) requires the agency to designate who the public can contact regarding inquiries about the justice information system or with whom complaints can be lodged. It also requires that contact information be provided to the public.

B.9.20 Accountability for Activities

(a) Primary responsibility for the operation of this justice information system—including operations; coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing, and disclosure of information; and the enforcement of this policy—is assigned to [*specify position responsible for the system*].

(b) The agency will establish procedures, practices, and system protocols and use software, information technology tools, and physical security measures that protect information from unauthorized access, modification, theft, or sabotage, whether internal or external and whether due to natural or human-caused disasters or intrusions. The methods and techniques used shall be consistent with [*provide reference to applicable technical standards or benchmarks specifying generally acceptable security practices*].

(c) The agency will store information in a manner such that it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions as provided in [*provide reference to applicable technical standards or benchmarks specifying generally acceptable information storage practices*].

(d) The agency will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users and the system itself with the provisions of this policy and applicable law. [*Consider referencing industry standards or generally accepted practices or adding language describing the mechanisms that will be used to ensure compliance, for example, adoption of information system security practices, logging of access requests and responses, and detection of unauthorized attempts to add, change, delete, or access information, audit practices, and other enforcement mechanisms.*]

(e) The agency will require any individuals authorized to use the system to agree in writing to comply with the provisions of this policy.

(f) The agency will periodically conduct audits and inspections of the information contained in the [*justice information system*]. The audits will be conducted randomly by a designated representative of the agency or by a designated independent party. The audit will be conducted in such a manner so as to protect the confidentiality, sensitivity, and privacy of the agency's information.

(g) The agency will periodically review and update the provisions protecting privacy, civil rights, and civil liberties in its policies and make appropriate changes in response to changes in applicable law and public expectations.

[*Consider adding: (h) The agency will notify an individual about whom unencrypted personal information was or is reasonably believed to have been obtained by an unauthorized person and access to which threatens*

physical 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 to reasonably restore the integrity of the information system. Notice need not be given if doing so meets the criteria specified in Subsection B.7.50 (b).]

Commentary

This section establishes the basic framework for holding the agency accountable for enforcing its privacy, civil rights, and civil liberties policy.

Subsection (a) requires the designation of an individual who is ultimately responsible for the operation of the system, in particular regarding privacy, civil rights, and civil liberties provisions.

Subsection (b) requires the agency to maintain and protect information in such a way that its integrity can be preserved and relied upon and to act to prevent unauthorized access, modification, or destruction of information. The information should be physically protected from improper access, intrusion, or destruction whether from humans or natural events. It should also be protected electronically through use of software, network, or other information technology tools. Assistance with both security concepts and implementation can be found in Applying Security Practices to Justice Information Sharing.[12] *The suggestion is made to cross-reference an industry standard or other statement of generally accepted practices covering the subjects of this subsection.*

Subsection (c) requires the agency to store information in a manner that minimizes the opportunity for someone to improperly access, modify, add to, or delete information. Storage refers equally to information in electronic or paper form. The suggestion made is to cross-reference an industry standard or other statement of generally accepted practices.

Subsection (d) requires the establishment of procedures and business practices that implement the intent of the privacy, civil liberties, and civil rights policy and that allow compliance with the policy to be effectively monitored. The language suggests adding a reference to specific approaches and techniques. The recitation of tools should increase public confidence that appropriate steps are being taken to protect information.

Subsection (e) requires users to sign a written agreement to comply with the policy provisions. This document can form a basis for enforcement actions (see Section B.9.30), whether personnel-related or criminal in nature. "Any individual" would include agency employees; employees of contractors and service providers who assist the agency in developing, maintaining, or using the system; and employees of other agencies authorized to use the system.

Subsection (f) requires periodic and random audits of the information held by the agency. The intent of an audit is both to act as a deterrent and to detect improper access to, retention of, or use of information. It can also reveal problems in data entry that create errors, whether random or systematic. All of these demonstrate public accountability and increase public confidence that the agency is acting responsibly.

Subsection (g) requires periodic review of the privacy and civil rights policy to ensure that it remains in compliance with applicable law, is responsive to changes in technology, and takes advantage of new technology that may assist in monitoring compliance and detecting violations of the privacy and civil rights policy. One way to ensure this is to consider the inclusion of a specific sunset date, thus forcing reevaluation of the effectiveness and scope of the policy.

---

12 Available at http://it.ojp.gov/documents/asp/.

Subsection (h) is proposed if the agency wants to commit itself to the type of notification of individuals required by law in several states where information held by an entity has been improperly released or disclosed. The unauthorized access ought to be brought to the attention of the individual so that they can take steps to protect themselves from harm. There is a requirement that the release could cause physical or financial harm to the individual, and there are exceptions intended to protect the integrity of the investigation and prosecution processes. The cross-reference to Subsection B.7.50 (b) refers to circumstances in which notice should not be given to a person because doing so might interfere with an existing investigation or potentially harm someone.

B.9.30 Enforcement

If a user is suspected of or found to be not complying with the provisions of this policy regarding the collection, use, retention, destruction, sharing, classification, or disclosure of information, the agency will:

(a) Suspend or discontinue access to information by the user;

(b) Suspend, demote, transfer, or terminate the person as permitted by applicable personnel policies;

(c) Apply other sanctions or administrative actions as provided in agency personnel policies;

(d) Request the agency, organization, contractor, or service provider employing the user to initiate proceedings to discipline the user or enforce the policy's provisions; or

(e) Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy as stated in [*Section B.1.00*].

Commentary

The policy will not adequately or effectively protect privacy, civil rights, or civil liberties if its provisions are violated with impunity. This section specifies the range of penalties for violations of the policy. Disciplinary action, appropriate to the severity of the offense, should be taken against a user who:

1) *Fails to comply with the provisions about what information may be sought or retained or what may not be sought or retained or who uses improper means or sources to seek or receive information;*
2) *Uses information for unauthorized purposes, including personal use or commercial use, whether or not the person receives a benefit;*
3) *Discloses information to someone not authorized to receive the information;*
4) *Fails to correct information found to be erroneous or to report the error to appropriate personnel;*
5) *Fails to purge information when it is no longer of value or has reached its retention schedule;*
6) *Retains or otherwise fails to destroy information that is scheduled to be destroyed or is no longer relevant to the purposes of the system; or*
7) *Fails to disclose information that an individual or the public is entitled to know the existence of and to review.*

Subsection (d) addresses the situation in which the user is not employed directly by the agency but is employed by or under contract to another entity that uses the system.

Training of agency employees, contractors, and users regarding the policy and consequences for violating it are addressed in Section B.10.00.

B.10.00 Training

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

- **(1) Its personnel;**
- **(2) Personnel providing information technology services to the agency;**
- **(3) Staff in other public agencies or private contractors providing services to the agency; and**
- **(4) Users who are not employed by the agency or a contractor.**

(b) The training program will cover:

- **(1) Purposes of the privacy, civil rights, and civil liberties protection policy;**
- **(2) Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the agency;**
- **(3) The impact of improper activities associated with information accessible within or through the agency; and**
- **(4) The nature and possible penalties for policy violations, including possible transfer, dismissal, civil and criminal liability, and immunity, if any.**

Commentary

Subsection (a) requires training not just of agency personnel but of others who may have access to information retained by the agency or that is accessible through the agency. The agency can require contractors to provide the necessary training as part of the contract with the agency. Users can be required to obtain the necessary training before being given authorization to access information retained by the agency.

Subsection (b) describes the subjects the training should encompass. It includes the basic aspects of the policy regarding privacy, civil rights, and civil liberties; why the policy is necessary; and the consequences for failing to comply with the policies. Consideration should also be given to establishing certification for the training, to encourage participation.

Subsection (b) (2) identifies the broad categories that should be covered in the training.

C. Provisions for a Multiagency Agreement for an Information Sharing System

This part contains suggestions for provisions that would be included in an interagency agreement between two or more governmental agencies establishing a justice information sharing system or network. The agencies involved could be local, state, tribal, territorial, federal, or international. The objective of the suggested provisions is to define the roles, responsibilities, and contributions of the agencies participating in the information sharing network relative to protection of privacy, civil rights, and civil liberties. These provisions should be included in the interagency agreement that is signed by the agencies who are participating in the justice information sharing system or network that defines its policies and operation. Any agency subsequently joining a justice information sharing system would also be expected to sign an interagency agreement containing these provisions.

The provisions suggested are stated in terms of principles, not details. The intent is that the interagency agreement state what is expected of the participating agencies regarding protection of privacy, civil rights, and civil liberties. How the participating agencies implement these protections internally is left to the agency, with the expectation that each agency's internal policies will address the requirements stated in the interagency agreement concepts. Adoption of a policy addressing the principles identified in Part B would presumably meet this requirement.

C.1.00 Statement of Purpose

The goal of establishing and maintaining this justice information sharing system is to further the following purposes:

(a) Increase public safety and improve national security;

(b) Minimize the threat and risk of injury to specific individuals;

(c) Minimize the threat and risk of injury to law enforcement and others responsible for public protection, safety, or health;

(d) Minimize the threat and risk of damage to real or personal property;

(e) Protect individual privacy, civil rights, civil liberties, and other protected interests;

(f) Protect the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information;

(g) Minimize reluctance of individuals or groups to use or cooperate with the justice system;

(h) Support the role of the justice system in society;

(i) Promote governmental legitimacy and accountability;

(j) Not unduly burden the ongoing business of the justice system; and

(k) Make the most effective use of public resources allocated to justice agencies.

Commentary

See Commentary under Section A.1.00 in Part A.

One justification for sharing information across agencies is that criminal activity and threats to public safety and health often occur across jurisdictional boundaries; thus sharing of information across jurisdictional boundaries is necessary to respond to these threats.

C.2.00 Compliance With Laws Regarding Privacy, Civil Rights, and Civil Liberties

The employees and users of the participating agencies and of the agency's information service providers will comply with all applicable laws protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing, and disclosure of information through the justice information sharing system.

Commentary

See Commentary under Section A.2.00 in Part A.

C.3.00 Sharing of Information Among Participants

C.3.10 Expectations Regarding Information Gathered and Shared

Participating agencies will adopt internal policies and procedures requiring the participating agency, its personnel, contractors, and users to:

(a) Only seek or retain information that is legally permissible for the agency to seek or retain under laws applicable to the 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) Take appropriate steps when merging information about an individual or organization from two or more sources to ensure that the information is about the same individual or organization;

(e) Investigate in a timely manner any alleged errors and correct or delete information found to be erroneous;

(f) 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, including terrorist, activities;

(g) Maintain information and systems containing information in a physically and electronically secure environment and protected from natural or man-made disasters or intrusions;

(h) Engage in collation and analysis of information in a manner that conforms to generally accepted practices;

(i) Establish procedures that comply with the policies and procedures of the justice information sharing system for accessing information through the participating agency;

(j) Only allow authorized users to access the information in the shared system and only for purposes related to the performance of their official duties;

(k) Share information with authorized users of other justice system partners based only on a "right-to-know" and a "need-to-know" basis; and

(l) Establish and comply with information retention and destruction schedules.

Commentary

The objective of this provision is to require participating agencies to adopt policies addressing the issues listed in this section. If an agency adopts a policy based on the provisions in Part B, they will be in compliance with these requirements when joining a justice information sharing system.

Expectations regarding the disclosure of information are provided for in Section C.4.10.

Compliance with and enforcement of the provisions adopted is addressed in Section C.5.00.

C.3.20 Sharing Information With Other Justice System Partners

A participating agency will make information available in response to a query either by:

(a) Providing the requested information directly;

(b) Responding with the contact information of a person in the responding agency whom the individual making the query can contact;

(c) Having a person in the responding agency contact the individual making the query; or

(d) Indicating that no information is available.

The choice of approach as to any particular piece of information shall be at the discretion of the agency that has retained the information.

Commentary

This provision gives a participating agency options regarding how to provide information in response to a query from another participating agency, thus providing an additional layer of protection for information and investigations. Most information from the responding agencies would be made available directly, either through a query to the agency's database or by a query to a data warehouse or a similar approach, to which participating agencies have transferred the information from their databases. If the agency queried desires a higher level of protection of the data, it can provide the person making the query with the contact information of someone in the responding agency. The person contacted can then verify the requestor's need to know and purpose of the inquiry before providing the information. This has the added benefit of letting the person in the responding agency know that others are interested in a particular individual, organization, or information. If the information is of a sensitive nature and not to be disclosed generally (for example, if it is part of an active investigation of a highly sensitive nature), the system could notify a designated contact in the agency that someone has made an inquiry and the decision can be made whether to call the person inquiring and what to disclose, if anything. Finally, the agency queried can simply decline to disclose information or respond that no information is available.

C.4.00 Use and Disclosure of Information Originating From Another Participating Agency

C.4.10 Disclosure of Information According to the Originating Agency's Access Rules

A participating agency will not disclose information originating from another agency except as [*authorized or required by law in the jurisdiction in which the information originated*] OR [*provided for in this agreement or in the operational policies of the shared information system*].

Commentary

This section provides two alternatives for the applicable policy regarding disclosure—either the policy of the agency that is the source of the information in the shared system or the disclosure policy of the justice information sharing system, whichever the participating agencies agree to. Alternatively, the language could state that the applicable policy is the most restrictive of the rules of the participating agencies.

If the provision requires participating agencies to follow the policy of the originating agency, two purposes are served. One is that it will encourage participating agencies to share information. If an agency is concerned that information will be disclosed in violation of its access policies, it may be unwilling to share the information. Second, it implements access and disclosure rules of the originating agency that are consistent with the circumstances and public expectation surrounding the collection of the information.

Implementation of this rule may not be as complicated as it may first appear. A user in another agency need not learn the access rules of the originating agency if an access category is associated with the information when it is included in the justice information sharing system, as required in Section B.4.40. The justice information sharing system will then provide access based on the access categorization.

C.4.20 Reporting Possible Information Errors to the Originating Agency

When a participating agency gathers or receives information that suggests that information originating from another agency may be erroneous, may include incorrectly merged information, or lacks relevant context, the alleged error will be communicated in writing to the person designated in the originating agency to receive such alleged errors pursuant to Subsection [*C.5.10 (e)*].

Commentary

The intent of this provision is both to improve the quality of the shared information and to make explicit the obligation of the person uncovering the possible error to report the alleged error back to the originating agency. Subsection C.3.10 (e) obligates the originating agency to investigate alleged errors reported to them and correct any errors found.

The obligation to communicate in writing is to increase the likelihood that something will be done by the receiving agency. Writing should include e-mail as well as any other form of writing; verbal communications should not be considered sufficient.

In order to implement this provision, each participating agency should identify a contact person to whom alleged errors are to be reported. This is required in Subsection C.5.10 (e).

C.5.00 Participating Agency Accountability and Enforcement

C.5.10 Expectations Regarding Accountability and Enforcement

Participating agencies will adopt and comply with internal policies and procedures requiring the agency, its personnel, contractors, and users to:

(a) Have and enforce policies for discovering and responding to violations of agency policies and this memorandum, including taking appropriate action when violations are found;

(b) Provide training to personnel authorized to use the justice information sharing network about the agency's requirements and policies regarding information collection, use, and disclosure;

(c) Make available to the public the agency's internal policies and procedures regarding privacy, civil rights, and civil liberties;

(d) Cooperate with periodic, random audits by representatives of the justice information sharing system; and

(e) Designate an individual within the participating agency to receive reports of alleged errors in the information that originated from the participating agency.

Commentary

The objective of this section is to explicitly state the need for participating agencies to monitor, conduct, and enforce policies regarding protection of privacy, civil rights, and civil liberties. Having a policy is meaningless if it can be ignored with impunity.

Subsection (e) requires each participating agency to identify a contact person to whom alleged errors are to be reported.

C.5.20 Enforcement of Provisions of Information Sharing Agreement

If a participating agency fails to comply with the provisions of this agreement or fails to enforce provisions in its local policies and procedures regarding proper collection, use, retention, destruction, sharing, disclosure, or classification of information, the justice information sharing network may:

(a) Suspend or discontinue access to shared information by a user in the offending agency who is not complying with the agreement or local policies and procedures;

(b) Suspend or discontinue the offending agency's access to the justice information sharing system; or

(c) Offer to provide an independent review, evaluation, or technical assistance to the participating agency to establish compliance.

Commentary

If a participating agency fails to comply with the law and policies protecting privacy, civil rights, and civil liberties, this section provides alternative responses. The subsections contain an escalating set of options designed to allow the information sharing system to protect information, yet retain the benefits of sharing. At the lowest level, the system terminates access by an offending user. If the problem is more pervasive in the agency, it can terminate access by the agency. Finally, there is the option of maintaining access but working with the agency to improve its practices and compliance.

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

The following federal laws should be reviewed when developing a privacy, civil rights, and civil liberties policy for a justice information system. The list is arranged in alphabetical order by popular name.

- **Brady Handgun Violence Prevention Act**, 18 U.S.C. §§ 921, 922, 924, and 925A, United States Code, Title 18, Part I, Chapter 44, §§ 921, 922, 924, and 925A
- **Computer Matching and Privacy Act of 1988**, 5 U.S.C. § 552a(a), United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a(a); see also Office of Management and Budget, Memorandum M-01-05, "Guidance on Interagency Sharing of Personal Data–Protecting Personal Privacy," December 20, 2000
- **Confidentiality of Identifiable Research and Statistical Information**, 28 CFR Part 22, Code of Federal Regulations, Title 28, Chapter I, Part 22
- **Criminal History Records Exchanged for Noncriminal Justice Purposes**, 42 U.S.C. § 14611, United States Code, Title 42, Chapter 140, Subchapter II, § 14611
- **Crime Identification Technology**, 42 U.S.C. § 14601, United States Code, Title 42, Chapter 140, Subchapter I, § 14601
- **Criminal Intelligence Systems Operating Policies**, 28 CFR Part 23, Code of Federal Regulations, Title 28, Chapter 1, Part 23
- **Criminal Justice Information Systems**, 28 CFR Part 20, Code of Federal Regulations, Title 28, Chapter 1, Part 20
- **Disposal of Consumer Report Information and Records**, 16 CFR Part 682, Code of Federal Regulations, Title 16, Chapter I, Part 682
- **Electronic Communications Privacy Act of 1986**, 18 U.S.C. §§ 2510–2522, 2701–2709, United States Code, Title 18, Part I, Chapter 119, §§ 2510–2522, 2701–2709, and 3121–3125, Public Law 99-508
- **Fair Credit Reporting Act**, 15 U.S.C. § 1681, United States Code, Title 15, Chapter 41, Subchapter III, § 1681
- **Federal Civil Rights** laws, 42 U.S.C. § 1983, United States Code, Title 42, Chapter 21, Subchapter I, § 1983
- **Federal Records Act**, 44 U.S.C. § 3301, United States Code, Title 44, Chapter 33, § 3301
- **Freedom of Information Act** (FOIA), 5 U.S.C. § 552, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552
- **Indian Civil Rights Act of 1968**, 25 U.S.C. § 1301, United States Code, Title 25, Chapter 15, Subchapter I, § 1301
- **HIPAA**, Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 201, United States Code, Title 42, Chapter 6A, Subchapter I, § 201; Public Law 104-191
- **HIPAA**, Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164; Code of Federal Regulations, Title 45, Parts 160 and 164
- **National Child Protection Act of 1993**, Public Law 103-209 (Dec. 20, 1993), 107 Stat. 2490
- **National Crime Prevention and Privacy Compact**, 42 U.S.C. § 14616, United States Code, Title 42, Chapter 140, Subchapter II, § 14616
- **Privacy Act of 1974**, 5 U.S.C. § 552a, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a

- **Privacy of Consumer Financial Information**, 16 CFR Part 313, Code of Federal Regulations, Title 16, Chapter I, Part 313
- **Protection of Human Subjects**, 28 CFR Part 46, Code of Federal Regulations, Title 28, Chapter 1, Volume 2, Part 46
- **Safeguarding Customer Information**, 16 CFR Part 314, Code of Federal Regulations, Title 16, Chapter I, Part 314
- **Sarbanes-Oxley Act of 2002**, 15 U.S.C., Chapter 98, § 7201, United States Code, Title 15, Chapter 98, § 7201
- **USA PATRIOT Act**, Public Law 107-56 (October 26, 2001), 115 Stat. 272
- **U.S. Constitution**, First, Fourth, and Sixth Amendments

Appendix Two
Local, State, Tribal, and Territorial Laws Possibly Relevant to Seeking, Retaining, and Disseminating Justice Information

Sources of Local, State, Tribal, and Territorial Laws:

The following local, state, tribal, and territorial laws should be reviewed when developing a privacy and civil rights policy for a justice information system:

- Constitution (in particular, provisions regarding information gathering, such as search and seizure)
- Statutes
- Regulations
- Court rules and procedural and practice rules
- Case law (federal and state)
- Attorneys Generals' opinions
- Executive orders and formal procedures and protocols
- Professional codes of ethics
- Local ordinances
- Tribal ordinances, resolutions, and descriptions of tribal customary laws
- Treaties

Specific Categories of Local, State, Tribal, and Territorial Laws to Review Regarding Seeking, Retaining, and Disseminating Justice Information:

- Access to criminal history or arrest information of applicants for caregiver positions
- Access to criminal history or arrest information of applicants for regulated professions
- Criminal history repository
- Integrated justice information system
- Criminal intelligence system
- Victim and witness protection
- Juveniles (in particular, regarding confidentiality of proceedings)
- Family relations laws (in particular, child custody and domestic violence)
- Medical records and information
- Civil harassment, restraining, and stay-away orders
- Civil commitments of individuals who pose a threat to themselves or others because of mental illness
- Public records acts (in particular, regarding justice system records and information)
- Open meeting laws as they affect the agency or the governing body of a justice information system

Activities or Events Subject to Local, State, Tribal, and Territorial Laws

The following list describes activities, events, transactions, and information exchanges that typically are the subject of justice information systems:

- Law enforcement contacts (in particular, traffic stops)
- Informants
- Surveillance, including pen registers and packet sniffers
- Search warrants
- Arrest warrants
- Arrests
- Interrogation
- Lineups
- Police logs
- Police reports (field reports, formal reports, and supplemental reports)
- Laboratory or forensic testing or analysis
- Investigation (existence, work products)
- Trial activities
- Information generated during a trial
- Victim-advocate logs
- Convictions (any distinctions based on seriousness of crime)
- Sentencing information, including programs providing alternatives to incarceration
- Treatment programs, including those imposed by problem-solving courts such as drug courts
- Probation (in particular, terms and conditions)
- Parole (in particular, terms and conditions)
- Domestic violence, civil harassment, and stay-away orders
- Enforcement of planning, zoning, environmental, and similar laws
- Other events, transactions, or activities revealed in the project's information exchange analysis

Appendix Three
Bibliography for Sources and References

Applying Security Practices to Justice Information Sharing, Global Justice Information Sharing Initiative Security Working Group, Version 4.0, May 2007, available at:

http://it.ojp.gov/documents/asp/

Developing CCJ/COSCA Guidelines for Public Access to Court Records: A National Project to Assist State Courts, Martha Wade Steketee and Alan Carlson, National Center for State Courts, October 18, 2002, available at:

http://www.courtaccess.org/modelpolicy/18Oct2002FinalReport.pdf or http://www.jmijustice.org/Data/DocumentLibrary/Documents/1141964905.77/CCJ-COSCA%20Access%2018Oct2002FinalReport.pdf

Fusion Center Guidelines, Developing and Sharing Information and Intelligence in a New Era, Global Justice Information Sharing Initiative, August 2006, available at:

http:it.ojp.gov/documents/fusion_center_guidelines.pdf

IACP Criminal Intelligence Model Policy, International Association of Chiefs of Police, June 2003.

IACP, *Criminal Intelligence Sharing: A National Plan for Intelligence-Led Policing at the Local, State, and Federal Levels*, International Association of Chiefs of Police, August 2002, available at:

http://www.theiacp.org/documents/pdfs/Publications/intelsharingreport.pdf

IACP Model Statutes Project: International Association of Chiefs of Police, revised October 2001.

Law Enforcement Analytic Standards, International Association of Law Enforcement Intelligence Analysts, Inc., November 2004.

IIR Sample Operating Policies and Procedures, Institute for Intergovernmental Research, (date unknown), available at:

http://www.iir.com/28cfr/SampleOperatingPolicies.pdf

Information Privacy: A Spotlight on Key Issues, National Association of State Chief Information Officers (NASCIO), February 2004, Version 1.0, available at:

https://www.nascio.org/publications/documents/NASCIO-InformationPrivacy2004.pdf

Information Quality: The Foundation for Justice Decision Making, Global Justice Information Sharing Initiative, Office of Justice Programs, U.S. Department of Justice.

http://it.ojp.gov/documents/IQ_Fact_Sheet_Final.pdf

NCISP Recommended Outreach Plan: *National Criminal Intelligence Sharing Plan*, Recommended Outreach Plan, July 2005.

National Criminal Intelligence Sharing Plan, Solutions and Approaches for a Cohesive Plan to Improve Our Nation's Ability to Share Criminal Intelligence, Global Justice Information Sharing Initiative, Office of Justice Programs, U.S. Department of Justice, issued October 2003, available at:

http://it.ojp.gov/documents/NCISP_Plan.pdf

Justice Information Privacy Guideline, Developing, Drafting and Assessing Privacy Policy for Justice Information Systems, National Criminal Justice Association, September 2002, available at

http://www.ncja.org/Content/NavigationMenu/PoliciesPractices/JusticeInformationPrivacyGuideline/default.htm

Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Annex to the Recommendation of the Council of 23rd September 1980, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Part Two. Basic Principles of National Application, available at

http://it.ojp.gov/process_links.jsp?link_id=4751

Privacy, Civil Liberties, and Information Quality Policy Development for the Justice Decision Maker, Global Justice Information Sharing Initiative, Office of Justice Programs, U.S. Department of Justice, February 2008, located at

http://it.ojp.gov/documents/global_privacy_brief.pdf

Privacy and Civil Liberties Policy Development Guide and Implementation Templates, Bureau of Justice Assistance, February 2008, available at

http://it.ojp.gov/documents/Privacy_Guide_Final.pdf

Privacy Technology Focus Group: Executive Summary, Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, slated for imminent release. Please call (850) 385-0600, extension 285, for further information.

RISS Privacy Policy: Regional Information Sharing Systems Privacy Policy, dated January 2004.

Safe Harbor Privacy Principles: U.S. Department of Commerce, issued July 21, 2000, available at

http://export.gov/safeharbor/SHPRINCIPLESFINAL.htm

SEARCH Compendium: *Compendium of State Privacy and Security Legislation: 2002 Overview, Criminal History Record Information*, Bureau of Justice Statistics, November 2003, NCJ 200030, available at

http://www.ojp.usdoj.gov/bjs/abstract/cspsl02.htm

Smith, Robert Ellis, *Compilation of State and Federal Privacy Laws*, the Privacy Journal, 2002, with 2004 Supplement, ISBN 0-930072-17-0, new 13-digit ISBN: 9780930072179, available through

http://www.privacyjournal.net/work1.htm

Appendix Four

Index of Subjects

References are to policy template sections and their associated commentary, not pages.

Appendix Five
Cross-Reference to Privacy-Related Laws and Other Policies

The following list provides references to laws, policies, and other statements of policy addressing policy issues similar to those addressed in the template sections here. They are provided as examples from comparable policy situations, even though many of these are not applicable to justice information systems. Bibliographic information for the references is provided in Appendix Three. The items listed under each section heading are in alphabetical order.

A. Elements of Enabling Legislation or Authorization

A.1.00 Statement of Purpose

- 16 CFR Part 314, Section 314.3(b)
- 28 CFR Part 20, Section 20.1
- 28 CFR Part 23, Sections 23.1 and 23.30(e)
- CCJ/COSCA Guidelines, Section 1.00
- *Fusion Center Guidelines*, Mission Statement and Goals, Guideline 2
- IIR Sample Operating Policies and Procedures, Goals

A.2.00 Compliance With Laws Regarding Privacy, Civil Rights, and Civil Liberties

- 28 CFR Part 23, Sections 23.1 and 23.2
- DOJ Order on Safeguarding Unclassified Sensitive Information, Section 6.f
- NCISP, Recommendations 6 and 9
- RISS Privacy Policy

A.3.00 Agency Transparency and Accountability

- NCISP, Recommendation 14
- NCISP Recommended Outreach Plan, generally

B. Elements of a Basic Internal Operations Policy

B.1.00 Statement of Purpose

- See References under Section A.1.00

B.2.00 Compliance With Laws Regarding Privacy, Civil Rights, and Civil Liberties

- See References under Section A.2.00

B.3.00 Definitions

B.3.10 Definition of Agency

- 28 CFR Part 23, Section 23.3(b)(4)
- DOJ Order on Safeguarding Unclassified Sensitive Information, Sections 2.a., 4.a., and 4.b

B.3.20 Definition of Information

- CCJ/COSCA Guidelines, Sections 3.10 and 3.40
- Computer Matching and Privacy Act, 5 U.S.C. § 552a(a)(4)

B.3.30 Definition of Law

- 28 CFR Part 20, Section 20.21(b)(2)

B.3.40 Definition of Public

- CCJ/COSCA Guidelines, Section 2.00

Other Definitions

Administration of Criminal Justice

- 28 CFR Part 20, Section 20.3(b)

Collect

- 16 CFR Part 313, Section 313.3(c)

Criminal Activity

- IIR Sample Operating Policies and Procedures, Definitions

Criminal History Record Information

- 28 CFR Part 20, Section 20.3(d)
- National Crime Prevention and Privacy Compact, 42 U.S.C. § 14616, Article I (4)

Criminal History Record Information System

- 28 CFR Part 20, Section 20.3(e)

Criminal Intelligence

- 28 CFR Part 23, Section 23.3(b)(1) and (3)
- IACP Model Policy, Section III
- *Law Enforcement Analytic Standards* definitions

Criminal Intelligence Information

- 28 CFR Part 23, Section 23.3(b)(3)
- IIR Sample Operating Policies and Procedures, Definitions

Criminal Intelligence System

- 28 CFR Part 23, Section 23.3(b)(1)
- IIR Sample Operating Policies and Procedures, Definitions

Dispose

- 16 CFR Part 682, Section 682.1(c)

Need to Know

- DOJ Order on Safeguarding Unclassified Sensitive Information, Section 4.e
- IIR Sample Operating Policies and Procedures, Definitions

Nonpublic Personal Information

- 16 CFR Part 313, Section 313.3(n)(1)

Personal Identifiable Financial Information

- 16 CFR Part 313, Section 313.3(o)(1)

Personal Identifiable Information

- Alaska Statutes, Section 44.99.350 (2)
- California Business and Professions Code, Section 22577(a) regarding Internet sites
- California Civil Code, Section 1798.81.5 (d)(1)—"personal information" in databases
- Federal Internal Revenue Service, 26 U.S.C. 6103(b)(6), definition of "Taxpayer information"
- Washington Governor's Executive Order 00-03
- Wisconsin Statutes, Sections 19.62(5)

Publicly Available Information

- 16 CFR Part 313, Section 313.3(p)(1)

Reasonable Suspicion

- 28 CFR Part 23, Section 23.20(c)
- IIR Sample Operating Policies and Procedures, Information Submission Criteria
- IIR Sample Operating Policies and Procedures, Definitions

Right to Know

- IIR Sample Operating Policies and Procedures, Definitions

B.4.00 Seeking and Retaining Information

B.4.10 What Information May Be Sought or Retained

Generally

- Computer Matching and Privacy Act, § 552a(e)(1)
- IACP Model Statutes Project, section on Racial Profiling
- OECD Collection Limitation Principle Number 7
- OECD Purpose Specification Principle Number 9
- RISS Privacy Policy
- Safe Harbor Privacy Principles, Notice, Choice, and Data Integrity principles
- Washington Governor's Executive Order 00-03, item #4

B.4.10 Subsection (a) (2) – Criminal History Information Systems

- 28 CFR Part 20, Section 20.3(d)
- Arizona Revised Statutes, Section 41-1750

B.4.10 Subsection (a) (3) – Criminal Intelligence Systems

- 28 CFR Part 23, Sections 23.20(a), (b), and (n) and 23.3(b)(3)
- IACP, Criminal Intelligence Model Policy, Sections II, IV.C.3. and IV.F.1
- IIR Sample Operating Policies and Procedures, Information Submission Criteria and Inquiry Procedures

B.4.10 Subsection (c) – Improper Basis for Collecting Information

- IACP Model Statutes Project, section on Racial Profiling

B.4.10 Subsection (c) – Information Not to Be Collected

- 28 CFR Part 23, Section 23.20(l)
- Computer Matching and Privacy Act, § 552a(e)(7)

B.4.20 Methods of Seeking or Receiving Information

- 28 CFR Part 23, Sections 23.20(d) and (k)
- Computer Matching and Privacy Act, § 552a(e)(2)
- IACP, Criminal Intelligence Model Policy, Section IV.C.2
- IACP Model Statutes Project, section on Racial Profiling
- IIR Sample Operating Policies and Procedures, Information Submission Criteria
- OECD Collection Limitation Principle Number 7
- OECD Purpose Specification Principle Number 9
- RISS Privacy Policy

B.4.30 Classification of Information Regarding Validity and Reliability

- 28 CFR Part 23, Sections 23.3(b)(6) [definition of "validation of information"] and 23.20(g)
- GSWG, *Applying Security Practices to Justice Information Sharing*, Section 2-4 Data Classification, pp. 2-43 to 2-47
- IALEIA, *Law Enforcement Analytic Standards*, Standard Number 13, Evaluation Standard
- IIR Sample Operating Policies and Procedures, section on Content Validity
- IIR Sample Operating Policies and Procedures, section on Source Reliability
- OECD Purpose Specification Principle Number 9

B.4.40 Classification of Information Regarding Limitations on Access and Disclosure

- DOJ Order on Safeguarding Unclassified Sensitive Information, Section 7.a
- IACP, Criminal Intelligence Model Policy provides classification categories for criminal intelligence information (see Section IV. H.1.)
- IALEIA, *Law Enforcement Analytic Standards*, Standard Number 23, Data Source Attribution Standard
- IIR Sample Operating Policies and Procedures, section on Dissemination Level
- OECD Purpose Specification Principle Number 9
- Safe Harbor Privacy Principles, Notice, Choice and Onward Transfer principles

B.5.00 Information Quality

Generally

- 20 CFR Part 20, Sections 20.1, 20.21(a) on completeness, 20.21(a)(2) on accuracy, 20.21(a)(2) on advising recipient agencies of errors, and 20.21(f)(3)(i)(a) on only authorized users changing data
- 28 CFR Part 23, Sections 23.20 (g) and (h)
- Computer Matching and Privacy Act, § 552a(e)(5) and (6)
- GSWG *Applying Security Practices to Justice Information Sharing*, Chapter 2, Section 3
- IIR Sample Operating Policies and Procedures, section on Notification Prior to Purge
- IALEIA, *Law Enforcement Analytic Standards*, Standard Number 12, Legal Constraints Standard, Standard Number 13, Evaluation Standard, and Standard Number 15, Analytic Accuracy Standard
- NCISP, Recommendations 11 and 12
- OECD Data Quality Principle Number 8
- Safe Harbor Privacy Principles, Data Integrity principle

B.6.00 Collation and Analysis of Information

B.6.10 Collation and Analysis

- IACP, Criminal Intelligence Model Policy, Sections IV. A. and E
- IALEIA, *Law Enforcement Analytic Standards*, Standard Number 14, Collation Standard
- NCISP, Recommendation 12

B.6.20 Merging of Information From Different Sources

- Colorado Rev. Stats., Section 24-72-305.4—Access to criminal history or arrest information for applicants for regulated professions—fingerprints for matching
- Computer Matching and Privacy Act, § 552a; definition of matching, § 552a(a)(8); matching agreement, § 552a(o); Data Integrity Boards, § 552a(u); law enforcement exception, § 552a(a)(8)(B)(iii), (v), and (vi)
- IIR Sample Operating Policies and Procedures, Information Submission Criteria
- Minnesota Statutes 2004, Chapter 13B—Matching Programs; Computerized Comparison of Data
- NASCIO Compendium, pp. 78-80
- National Crime Prevention and Privacy Compact, 42 U.S.C. § 14616, Article I (20) "positive identification," Article V (a), and Article V (e)
- Wisconsin Statutes, Sections 19.62(3) [definition of matching program] and 19.69

B.6.20 Subsection (b) – Independent Verification of Match

- Minnesota Statutes 2004, Section 13B.03
- Wisconsin Statutes, Section 19.67(b)

B.7.00 Sharing and Disclosure of Information

- Dissemination according to applicable laws
  - Florida Statutes, Section 934.053(1)

B.7.10 Sharing Information Within the Agency and With Other Justice System Partners

- 28 CFR Part 20, Sections 20.21(b)(1), (b)(3), (f)(2), and (f)(3)(i)(b), and Section 20.33(a)
- 28 CFR Part 23, Sections 23.20(e), (f), and (g)
- Florida Statutes Section 943.053(6) to public defenders
- Florida Statutes Section 943.053(7) to private entities contracting with a sheriff to run a detention facility; 943.053(8) to private entities operating correctional facilities for the state; and 943.053(9) to contracted juvenile assessment center or detention facility
- GSWG *Applying Security Practices to Justice Information Sharing*, Chapter 2, Section 2
- IACP Criminal Intelligence Model Policy, Section IV. C.4
- IIR Sample Operating Policies and Procedures, sections on Access Rights, Inquiry Procedures, and Dissemination of Information Procedures
- NCISP, Recommendation 27
- OECD Use Limitation Principle Number 10
- OECD Security Safeguards Principle Number 11
- Safe Harbor Privacy Principles, Onward Transfer principle

B.7.20 Sharing Information With Those Responsible for Public Protection, Safety, or Public Health

- 28 CFR Part 20, Sections 20.21(b)(2) and 20.33(a)

- 28 CFR Part 23, Sections 23.20 (f)(2) and (g)
- OECD Use Limitation Principle Number 10
- OECD Security Safeguards Principle Number 11
- Safe Harbor Privacy Principles, Inward Transfer principle

B.7.30 Sharing Information for Specific Purposes

- 28 CFR Part 20, Sections 20.21(b)(2) and (c)(1) on specific users and information they are entitled to access, and 20.21(b) (4) on research, evaluation and statistical uses
- 28 CFR Part 20, Section 20.21(c)(2) on nondisclosure of existence of information
- 28 CFR Part 20, Section 20.33(a) on information made available for specific uses
- 28 CFR Part 23, Section 23.20(f)(2) and (g)
- CCJ/COSCA Guidelines, Section 4.10
- National Crime Prevention and Privacy Compact, 42 U.S.C. § 14616, Article IV (a)
- OECD Use Limitation Principle Number 10
- OECD Security Safeguards Principle Number 11

B.7.30 Access to Criminal History or Arrest Information for Applicants for Caregiver Positions

- Colorado Rev. Stats., Section 24-72-305.3 (2)(B)–clear language about what types of criminal information is available

B.7.30 Access to Criminal History or Arrest Information for Applicants for Regulated Professions

- Colorado Rev. Stats., Section 24-72-305.4; use of fingerprints for matching in Subsection (1)
- Safe Harbor Privacy Principles, Inward Transfer principle

B.7.30 Access to Criminal Records Information for Child Support Enforcement Agency

- Florida Statutes Section 943.053(5)

B.7.40 Disclosing Information to the Public

- 28 CFR Part 20, Section 20.20(b) on exceptions and 20.20(c) on disclosing criminal history information about an individual
- 28 CFR Part 23, Section 23.20(g)
- Federal Freedom of Information Act, 5 U.S.C. Section 552 (b) on exceptions to disclosure
- Federal Freedom of Information Act, 5 U.S.C. Section 552(a)(2) on redaction and disclosing existence of information not made available
- Florida Statutes Section 119.07(1)(b) and (c)—redaction of exempt portion of record and citation of authority to not provide
- New Jersey Statutes, Section 47:1A-3.b
- OECD Use Limitation Principle Number 10
- OECD Security Safeguards Principle Number 11
- Safe Harbor Privacy Principles, Onward Transfer and Security principles
- Washington Governor's Executive Order 00-03, item #3
- Wisconsin Statutes, Section 19.71 – sale of names and addresses

B.7.40 Subsection (d)—Fees for Obtaining Information

- CCJ/COSCA Guidelines, Section 4.30 and 4.40 on bulk and compiled access and Section 6.00 on fees
- Federal Freedom of Information Act, 5 U.S.C. Section 552(a)(4) on charging fees

B.7.40 Subsection (e)—Bulk Access to Information

- CCJ/COSCA Guidelines, Sections 4.30 and 4.40

B.7.50 Disclosing Information to the Individual About Whom Information Has Been Gathered

- 28 CFR Part 16, Sections 16.30 – 16.34
- 28 CFR Part 20, Sections 20.21(g) and 20.34
- 28 CFR Part 23, Section 23.20 (g)
- Computer Matching and Privacy Act, § 552a Subsections (e)(3) and (f)
- Fair Credit Reporting Act
- New Jersey Statutes, Section 47:1A-3.a
- OECD Individual Participation Principle Number 13
- Safe Harbor Privacy Principles, Notice, Choice and Access principles

B.7.50 Subsection (c)—Review and Correction

- Computer Matching and Privacy Act, § 552a (p)

B.8.00 Information Retention and Destruction

B.8.10 Review of Information Regarding Retention

- 28 CFR Part 23, Section 23.20(h)
- IIR Sample Operating Policies and Procedures, section on Review and Purge Procedures
- RISS Privacy Policy
- Washington Governor's Executive Order 00-03, item #4

B.8.20 Destruction of Information

- 16 CFR Part 682, Section 682.3
- Federal Records Act, 44 U.S.C. Chapter 33, Sections 3303 (3) and 3303a (d)
- IIR Sample Operating Policies and Procedures, sections on Review and Purge Procedures, Procedures for Purge of Information, Purge Without Notification to Submitting Agency, Notification Prior to Purge, and Destruction of Information
- RISS Privacy Policy

B.9.00 Accountability and Enforcement

B.9.10 Information System Transparency

Generally:

- NCISP Recommended Outreach Plan
- OECD Openness Principle Number 12

B.9.10 Subsection (a)—Existence of System

- Computer Matching and Privacy Act, § 552a, Subsections (e)(4), (11) and (12) and Subsection (r)

B.9.10 Subsection (b)—Designating Responsible Person:

- 16 CFR Part 314, Section 314.4(a)
- Executive Order 12334 – President's Intelligence Oversight Board, Section 2
- IACP Criminal Intelligence Model Policy, Section IV.B.2—concept of "officer-in-charge" (OIC)
- IIR Sample Operating Policies and Procedures, Coordination and Control

- OECD Accountability Principle Number 14

B.9.20 Accountability for Activities

- 16 CFR Part 314, Section 314.4(b)
- 28 CFR Part 20, Sections 20.21(e) on audits, (f) on security provisions, (f)(3)(i)(a) on who can change information, (f)(3)(i)(d) on detecting attempted unauthorized use, and (f)(3)(i)(g) on protecting the system
- 28 CFR Part 23, Sections 23.20(g), (i), and (n), and 23.30(c) and (d)(1)
- Computer Matching and Privacy Act, § 552a(e)(9)
- IACP, Criminal Intelligence Model Policy, Section IV.B
- IIR Sample Operating Policies and Procedures, section on Inspection and Audit of Files
- National Crime Prevention and Privacy Compact, 42 U.S.C. § 14616, Article III (a)(1) and (b)(1)
- NCISP, Recommendation 15
- RISS Privacy Policy
- Safe Harbor Privacy Principles, Enforcement principle

B.9.20 Subsection (a)—Person/Position Responsible

- DOJ Order on Safeguarding Unclassified Sensitive Information, Sections 5.c. and 6.h

B.9.20 Subsection (b)—Protection From Destruction or Unauthorized Access

- GSWG *Applying Security Practices to Justice Information Sharing*

B.9.20 Subsection (d)—Compliance and Subsection f) – Audit

- 16 CFR Part 314, Section 314.4(c)
- Computer Matching and Privacy Act, § 552a (u)(3)(B)
- Washington Governor's Executive Order 00-03, item #5
- Wisconsin Statutes, Section 19.65(2)—Rules of conduct for employees

B.9.20 Subsection (g)—Updating of Policy

- DOJ Order on Safeguarding Unclassified Sensitive Information, Section 8

B.9.20 Subsection (h)—Notification of Breach and Release of Information

- California

B.9.30 Enforcement

- 28 CFR Part 20, Section 20.21(f)(4)(ii)
- 28 CFR Part 23, Sections 23.20(g)(5) and (m)
- Computer Matching and Privacy Act, § 552a(q)
- DOJ Order on Safeguarding Unclassified Sensitive Information, Section 5.b
- Federal Freedom of Information Act, 5 U.S.C. Section 552 (a)(4)(F)
- Safe Harbor Privacy Principles, Enforcement principle
- Washington Governor's Executive Order 00-03, item #5
- Wisconsin Statutes, Section 19.80

B.10.00 Training

- 28 CFR Part 20, Section 20.21(f)(5)
- CCJ/COSCA Guidelines, Section 8.30
- Computer Matching and Privacy Act, § 552a(e)(9)
- DOJ Order on Safeguarding Unclassified Sensitive Information, Section 5.b

- IACP Model Statutes Project, section on Racial Profiling
- IALEIA, *Law Enforcement Analytic Standards*
- NCISP, Recommendations 13, 18, and 19
- Washington Governor's Executive Order 00-03, item #5
- Wisconsin Statutes, Section 19.65

C. Provisions for a Multiagency Agreement for an Information Sharing System

C.1.00 Statement of Purpose

- See References under Section A.1.00

C.2.00 Compliance With Laws Regarding Privacy, Civil Rights, and Civil Liberties

- See References under Section A.1.00
- 28 CFR Part 23, Sections 23.1 and 23.2
- National Crime Prevention and Privacy Compact, 42 U.S.C. §14616, Article III (c)
- RISS Privacy Policy

C.3.00 Sharing of Information Among Participants

C.3.10 Expectations Regarding Information Gathered and Shared

- 28 CFR Part 20, Sections 20.21(a), 20.21(f)(3)(i)(f) and (f)(3)(i)(g), and 20.37
- 28 CFR Part 23, Sections 23.20(e) and (h) and 23.30(d)(2)
- IIR Sample Participation Agreement
- National Crime Prevention and Privacy Compact, 42 U.S.C. Section 14616, especially Article III (c)

C.3.10 Subsection (g)—System Security

- For a summary of security provisions, see IIR Sample Operating Policies and Procedures, section on Security of SIS Files

C.3.10 Subsections (i), (j) and (k)

- *Applying Security Practices to Justice Information Sharing*, Chapter 2, Section 2

C.3.20 Sharing Information With Other Justice System Partners

- IIR Sample Operating Policies and Procedures, section on Dissemination Level

C.4.00 Use and Disclosure of Information Originating From Another Participating Agency

C.4.10 Disclosure of Information According to Originating Agencies Access Rules

- Florida Statutes, Sections 119.071(2)(b) and 934.053(2)
- IIR Sample Operating Policies and Procedures, Section on Dissemination Level
- Washington Governor's Executive Order 00-03, item #5

C.4.20 Reporting Possible Information Errors to the Originating Agency

- 28 CFR Part 23, Section 23.20 (h)

C.5.00 Participating Agency Accountability and Enforcement

C.5.10 Expectations Regarding Accountability and Enforcement

- IIR Sample Operating Policies and Procedures, section on Inspection and Audit of Files
- IIR Sample Operating Policies and Procedures, Participation—on designated contact person for receiving reports of alleged errors
- National Crime Prevention and Privacy Compact, 42 U.S.C. § 14616, Article II (5), Article III (c), and Article IV (c)

C.5.20 Enforcement of Provisions of Information Sharing Agreement

- 28 CFR Part 20, Section 20.38