U.S. Department of Justice's
Global Justice Information Sharing Initiative

Global Justice Information Sharing Initiative

United States
Department of Justice

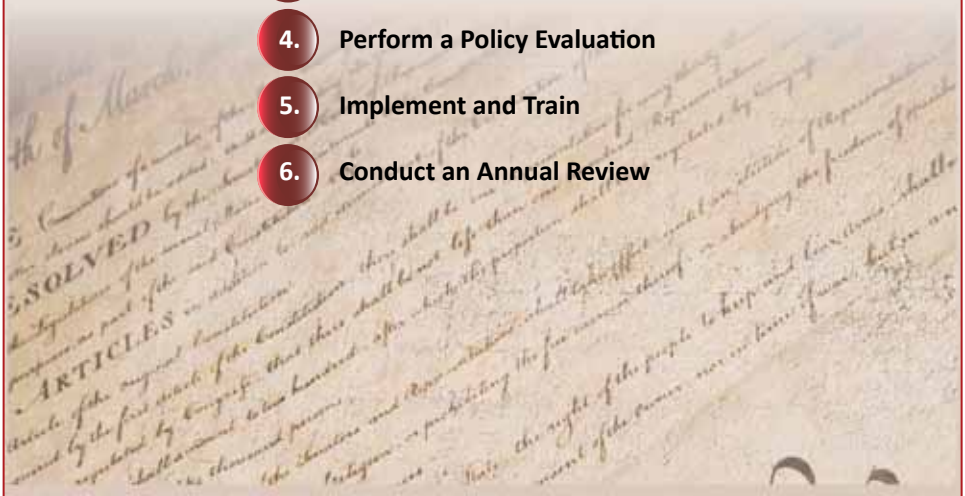
Global Privacy Resources

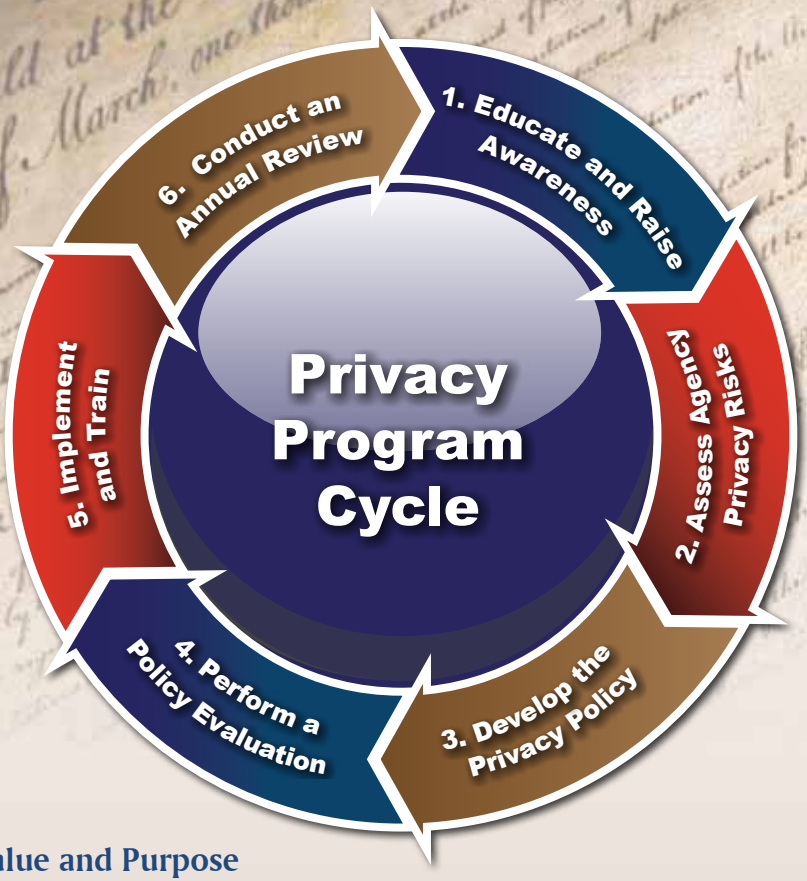
Global Privacy Resources

To support justice agencies in their efforts to implement privacy, civil rights, and civil liberties policies and protections for the information they collect, store, maintain, access, share, and disseminate, the U.S. Department of Justice's (DOJ) Global Justice Information Sharing Initiative (Global) has published this *Global Privacy Resources* document as a road map to guide justice entities through the diverse privacy policy development and implementation products available today. The resources presented here were developed for state, local, and tribal (SLT) entities by DOJ's Global or Global partners or through DOJ collaborations with other federal agencies, such as the U.S. Department of Homeland Security (DHS).

Global recognizes that SLT justice entities come in all sizes, with a variety of roles and with varying degrees of available resources. This document was developed to illustrate the flexible suite of products available for every stage of an entity's privacy program cycle, each designed to meet a spectrum of privacy protection needs:

1. **Educate and Raise Awareness**
2. **Assess Agency Privacy Risks**
3. **Develop the Privacy Policy**
4. **Perform a Policy Evaluation**
5. **Implement and Train**
6. **Conduct an Annual Review**





Value and Purpose

Justice agencies are encouraged to use the resources described here to ensure that privacy, civil rights, and civil liberties protections are in place for the information in their justice systems. Such protections will reduce risks to public safety, reduce legal liability of justice entities, and uphold a justice entity's reputation. Protecting privacy, civil rights, and civil liberties through the course of everyday justice work inspires trust in the justice system and in the law enforcement entities that collect and use this information.

Where to Locate These Resources

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

Stage 1 Educate and Raise Awareness

These resources will familiarize agency administrators with the importance of having privacy, civil rights, and civil liberties protections within their agency and will provide a high-level overview of the seven steps an agency should follow to develop a privacy policy.

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

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

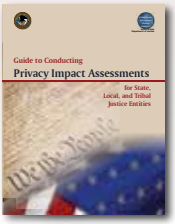
- ***7 Steps to a Privacy, Civil Rights, and Civil Liberties Policy***

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

Stage 2 Assess Agency Privacy Risks

Understanding agency privacy risks is critical to the development of a privacy policy that establishes how an agency collects, maintains, and shares agency justice information.

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



Practitioners are provided a framework with which to examine the privacy implications of their information systems and information sharing collaborations so they can design and implement privacy policies to address vulnerabilities identified through the assessment process. Privacy policies emerge as a result of the analysis performed during the Privacy Impact Assessment (PIA) process. In addition to an overview of the PIA process, this guide contains a template that leads policy developers through a series of appropriate PIA questions that evaluate the process through which personally identifiable information is collected, stored, protected, shared, and managed. The PIA questions are designed to reflect the same policy concepts as those recommended in the *Privacy, Civil Rights, and Civil Liberties Policy Development Guide for State, Local, and Tribal Justice Entities*, featured in Stage 3, further supporting privacy policy development.

Stage 3 Develop the Privacy Policy

After a Privacy Impact Assessment is completed, the next stage is the development of policies to address privacy, civil rights, and civil liberties vulnerabilities.

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

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

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

  Included in the Privacy Guide is the SLT Policy Development Template, which was developed to assist SLT agencies in drafting a privacy policy. The provisions suggested are intended to be incorporated into the agency's general operational policies and day-to-day operations. Each section represents a fundamental component of a comprehensive policy that includes baseline provisions on information collection, information quality, collation and analysis, merging, access and disclosure, redress, security, retention and destruction, accountability and enforcement, and training. Sample language is included for each provision.

- ***Fusion Center Privacy Policy Development: Privacy, Civil Rights, and Civil Liberties Policy Template* (FC Privacy Template)**

  The FC Privacy Template was developed by DOJ in collaboration with the U.S. Department of Homeland Security (DHS) in the joint DHS/DOJ Fusion Process Technical Assistance Program. This template was designed specifically to assist fusion center personnel in developing a privacy policy related to the information, intelligence, and suspicious activity report (SAR) information the center gathers, collects, receives, maintains, archives, accesses, discloses, and disseminates to center personnel, governmental agencies, Information Sharing Environment (ISE) participants, and other participating criminal justice and public safety agencies, as well as to private contractors and the general public. Provisions contained in this template help centers comply with requirements of the DHS Homeland Security Grant Program Guidance, the ISE Privacy Guidelines, and the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI).

- **Online Repository of Fusion Center Privacy, Civil Rights, and Civil Liberties Protections Policies**

  An additional policy development resource for those agencies with an intelligence function is an online repository of fusion center privacy policies, hosted by the National Fusion Center Association, www.nfcausa.org. Each policy posted on this site has met all of the criteria outlined in the *Fusion Center Privacy Policy Development: Privacy, Civil Rights, and Civil Liberties Policy Template* (described above) and has been determined by the DHS Privacy Office to be "at least as comprehensive as the Information Sharing Environment (ISE) Privacy Guidelines." These policies are the result of the joint DHS/DOJ Fusion Process Technical Assistance Program.

- **Information Sharing Environment Privacy Guidelines Implementation Support**

  In collaboration with the Bureau of Justice Assistance (BJA) and the Office of the Program Manager for the Information Sharing Environment (PM-ISE), this program provides support to assist federal agencies in the ongoing implementation of the *Guidelines to Ensure That the Information Privacy and Other Legal Rights of Americans Are Protected in the Development and Use of the Information Sharing Environment* (ISE Privacy Guidelines). Privacy technical assistance is provided to federal agencies in the development of privacy policies that comply with the ISE Privacy Guidelines. For more information on this program, refer to www.ise.gov/privacy-civil-rights-and-civil-liberties-protection-framework.

Stage 4 Perform a Policy Evaluation

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

- ***Policy Review Checklist***

The checklist is a companion piece to the SLT Policy Development Template, described in Stage 3, and serves both as a self-assessment tool to assist privacy policy authors, project teams, and agency administrators in evaluating whether the provisions contained within their draft policy have met the core concepts recommended in the SLT Policy Development Template, as well as a useful resource for the annual policy review, recommended in Stage 6. The checklist is structured according to policy provision categories. These include key concepts such as:

  - Policy applicability and legal compliance
  - Governance and oversight
  - Acquiring and receiving information
  - Information quality assurance
  - Sharing and dissemination
  - Redress
  - Security safeguards
  - Information retention and destruction
  - Accountability and enforcement

Section references are also provided to correlate checklist components with those in the SLT Policy Development Template.

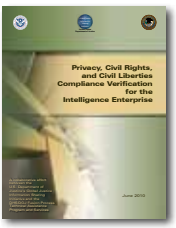
Stage 5 Implement and Train

After the privacy policy is finalized, the entity will next **implement** the policy requirements systematically and train personnel and authorized users on the established rules and procedures.

- ***Implementing Privacy Policy in Justice Information Sharing: A Technical Framework***

This resource was developed for technical practitioners to provide guidelines for supporting the electronic expression of a privacy policy and how to convert a privacy policy so that it is understandable to computers and software. A technical framework provides approaches and alternatives to resolving technical and interoperability challenges in supporting a privacy policy through automation. It outlines a sequence of steps for implementing a set of electronic privacy policy rules that can be readily implemented using existing information technology architectures, standards, and software tools. To view this document, refer to www.it.ojp.gov/privacy-technical-framework.pdf. An executive summary is also available at www.it.ojp.gov/documents/Privacy_policy_flyer.pdf.

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

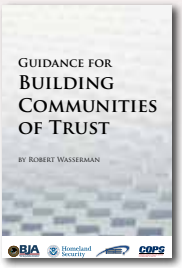


This compliance verification document assists intelligence enterprises in complying with all applicable privacy, civil rights, and civil liberties protection laws, regulations, and policies. As a "next step" for agencies that have completed and implemented protections established in the privacy policy, the checklist evaluates agency compliance with the policies and procedures and helps to uncover any gaps that may need to be addressed. The checklist provides a suggested methodology for conducting the review of an agency's intelligence enterprise and identifies the high-liability areas of concern

that should be included when performing the review. This resource is being used for ongoing peer-to-peer assessment at multiple fusion centers, and a best practices document resulting from the peer reviews is forthcoming. To view this document, refer to www.ncirc.gov/documents/public/supplementaries/privacy_verification.pdf.

Another area of implementation is the **liaison** of justice entities with the communities they serve to inform them of the thoughtful, intentional process used to develop privacy protections and to promote public confidence in the justice entity and in the safety and integrity of the information contained in justice systems.

- ***Guidance for Building Communities of Trust***



This resource, developed by Robert Wasserman in collaboration with the Office of Community Oriented Policing Services (COPS), DOJ, and DHS, focuses on developing relationships of trust among law enforcement, fusion centers, and the communities they serve, particularly immigrant and minority communities, to address the challenges of crime control and prevention of terrorism. Trust, transparency, and the protection of privacy, civil rights, and civil liberties are fundamental to effective crime control, and these principles must serve as the foundation for information and intelligence sharing efforts intended to support crime prevention and terrorism prevention activities. The objective of this resource is to help communities understand how law enforcement is using information to protect neighborhoods and citizens, while at the same time educate law enforcement on the priorities and needs of residents and how various community members view law enforcement efforts. This guide provides advice and recommendations on how to initiate and sustain trusting relationships that support meaningful sharing of information, responsiveness to community concerns and priorities, and the reporting of suspicious activities. Building and maintaining trusting relationships between communities and law enforcement to prevent acts of crime and terrorism is the overarching theme of this document. To view this resource, refer to www.cops.usdoj.gov/files/RIC/Publications/e071021293_buildingcommtrust_revision.pdf.

Training is essential to the effective implementation of any privacy policy. In addition to the two awareness primers described in Stage 1, the following resources are available for training purposes.

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

  This short video was developed as a training tool to educate viewers, particularly line officers during roll call, on the privacy and civil liberties issues they may confront in their everyday work. The video also addresses the liabilities associated with the failure to adhere to sound policy and practice. This short overview reviews and proactively emphasizes the role line officers have in the ongoing protection of citizens' and community members' privacy, civil rights, civil liberties, and other associated rights in the course of officers' daily activities and calls for service. This video can be viewed online at www.ncirc.gov/privacylineofficer/.

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

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

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

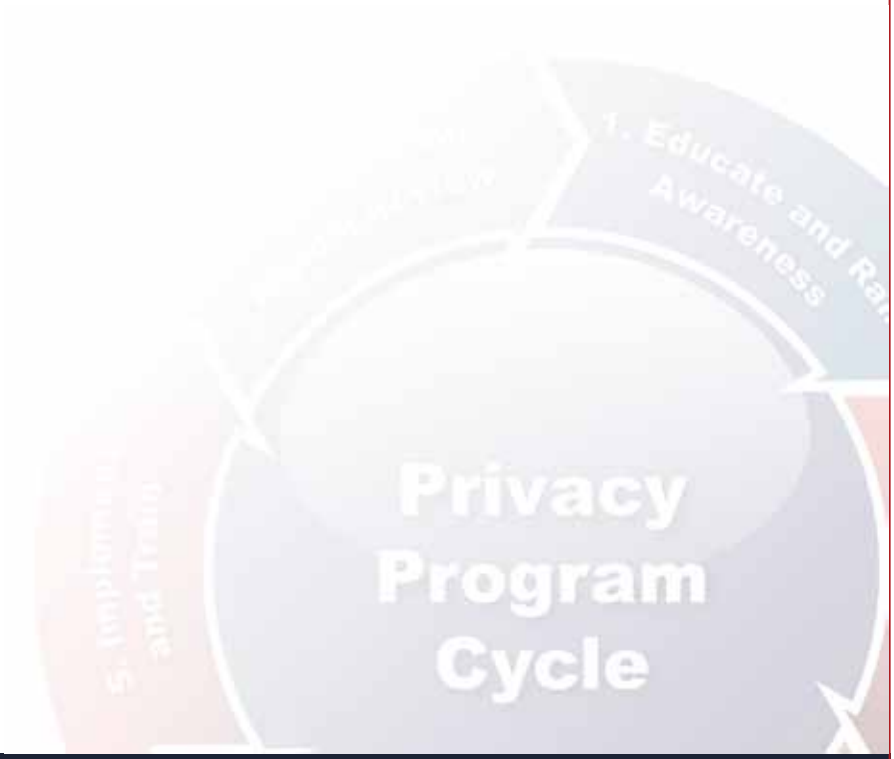
Criminal intelligence plays a vital role in the safety and security of our country. The Code of Federal Regulations, Title 28, Part 23—Criminal Intelligence Systems Operating Policies (or 28 CFR Part 23) was issued in 1980 to ensure the privacy and constitutional rights of individuals during the collection and exchange of criminal intelligence information, and it has since been an important part of the intelligence landscape. 28 CFR Part 23 is a guideline for law enforcement agencies that operate federally funded multijurisdictional criminal intelligence systems. To facilitate greater understanding of 28 CFR Part 23, the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, developed the Criminal Intelligence Systems Operating Policies (28 CFR Part 23) online training, which focuses on the requirements of 28 CFR Part 23 and includes topics such as compliance, privacy, inquiry, and dissemination requirements; storage requirements; and review-and-purge requirements. The online training is available at www.ncirc.gov or www.iir.com/Justice_Training/28cfr/default.aspx.

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

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

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

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



Stage 6 Conduct an Annual Review

Applying the guidance described in the Privacy Guide featured in Stage 3, justice entities are encouraged to review and update the provisions protecting privacy, civil rights, and civil liberties contained in the privacy policy at least **annually** using the annual review section of the *Policy Review Checklist* referenced in Stage 4. This update will ensure that appropriate changes are made in response to changes in applicable laws, technology, the purpose and use of the information systems, and public expectations. Once the policy is updated, entities should revisit the resources listed in each stage of the privacy program cycle. This will ensure that systems and individuals comply with the most current protections established in the entity privacy policy.

About Global

www.it.ojp.gov/global

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

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

About GPIQWG

www.it.ojp.gov/privacy

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

GPIQWG, on behalf of DOJ's Global, developed this overview to support justice agencies in their efforts to establish and implement an agency-wide privacy program. For more information on GPIQWG or to view resources listed within this publication, refer to: www.it.ojp.gov/privacy.

BJA
Bureau of Justice Assistance
U.S. Department of Justice

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

Issued 07/11