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

Global Justice Information Sharing Initiative

## Guide to Conducting

# Privacy Impact Assessments

### for State, Local, Tribal, and Territorial (SLTT) Justice Entities

Version 2.0
August 2020

**Where to Locate These Resources**

The Global Privacy Resources featured within this guide and others are available online at www.it.ojp.gov/privacy. To request printed copies, send requests to GLOBAL@iir.com.

**About the Global Advisory Committee**

**www.it.ojp.gov/global**

The Global Advisory Committee (GAC) serves as a Federal Advisory Committee to the U.S. Attorney General. Through recommendations to the Bureau of Justice Assistance (BJA), the GAC supports standards-based electronic information exchanges that provide justice and public safety communities with timely, accurate, complete, and accessible information, appropriately shared in a secure and trusted environment. GAC recommendations support the mission of the U.S. Department of Justice, initiatives sponsored by BJA, and related activities sponsored by BJA's Global Justice Information Sharing Initiative (Global). BJA engages GAC member organizations and the constituents they serve through collaborative efforts, such as Global working groups, to help address critical justice information sharing issues for the benefit of practitioners in the field.

This project was supported by Grant No. 2014-DB-BX-K004 awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, in collaboration with the Global Justice Information Sharing Initiative. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the U.S. Department of Justice.

# Table of Contents

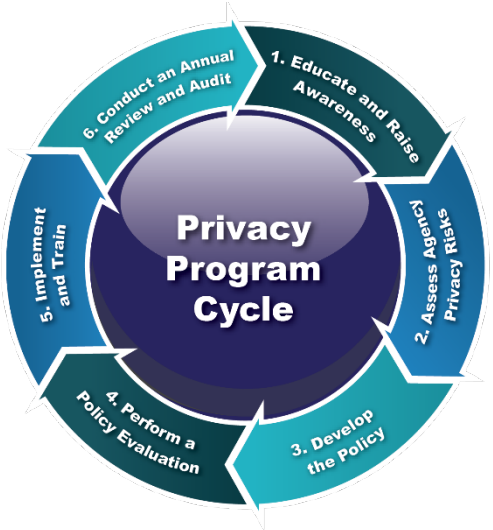
**This page intentionally left blank**.

# Introduction

This *Guide to Conducting Privacy Impact Assessments for State, Local, Tribal, and Territorial Justice Entities* (or "PIA Guide") allows practitioners at state, local, tribal, and territorial (SLTT) justice entities to examine the privacy implications of their information systems and information sharing collaborations so they can design and implement policies to address vulnerabilities identified through the assessment process.

The Global Justice Information Sharing Initiative (Global) develops resources to support justice entities in their efforts to develop and implement privacy, civil rights, and civil liberties policies and protections in their information sharing initiatives.

## I. Privacy Program Cycle




Global has developed a flexible suite of products for every stage of an entity's privacy program cycle, each designed to meet a spectrum of privacy protection needs.

**Stage 1—Educate and Raise Awareness** on the importance of having privacy, civil rights, and civil liberties (P/CRCL) protections within the agency.

**Stage 2—Assess Agency Privacy Risks** by evaluating the process through which your agency collects, stores, protects, shares, and manages information.

**Stage 3—Develop the Policy** to articulate an organization's policy position on how it handles information it seeks or receives and uses in the normal course of business.

**Stage 4—Perform a Policy Evaluation** to determine whether the P/CRCL policy adequately addresses current standards and privacy protection recommendations.

**Stage 5—Implement and Train** personnel and authorized users on the established rules and procedures.

**Stage 6—Conduct an Annual Review and Audit** and make appropriate modifications to reflect changes in applicable laws, technology, public expectations, and implementation experience, including the results of periodic audits and inspections.

This PIA Guide serves as the primary resource for Stage 2—Assess Agency Privacy Risks. Applying the privacy principles and practices discussed in the Global *Privacy, Civil Rights, and Civil Liberties Policy Development Guide for State, Local, Tribal, and Territorial Justice Entities* (P/CRCL Policy Development Guide), the PIA Guide helps an entity prepare for drafting a P/CRCL policy by identifying privacy risks associated with its information sharing systems. Once an entity completes a PIA, the entity is encouraged to refer to resources at **Stage 3—Develop the P/CRCL policy for tools to assist in the policy development process. For more information on all of the privacy resources available for each stage of an entity's Privacy Program Cycle, refer to www.it.ojp.gov/privacy.**

## II. Background

Information may be the wild card in the justice enterprise deck. Its expanded utility, made possible in large part by advances in information technology, strengthens public safety and supports the development and growth of SLTT and regional justice information sharing initiatives.

However, inappropriate or reckless use of information can cause demonstrable harm by irreparably damaging reputations, threatening individual liberty, placing personal safety at risk, or denying individuals access to some of life's most basic necessities, such as employment, housing, and education.

Justice entity pursuit of information sharing capabilities must be accompanied equally by responsibility for ensuring the privacy, civil rights, and civil liberties protections of the information being used and exchanged.

Information is maximized to its full potential only when it is used in the most responsible manner possible. This requires carefully designed privacy protections that reflect not only the tremendous benefits that information sharing can provide but also the damages that can occur when information is used and exchanged in a manner that conflicts with common expectations of privacy and confidentiality.

While the E-Government Act of 2002[1] resulted in significant federal-level P/CRCL policy activity, particularly in PIA use for new or significantly modified federal information technology (IT) systems, there has been little activity on the state, local, or tribal fronts in P/CRCL policy development or PIA use to examine IT system privacy vulnerabilities.

This risk assessment—more commonly known as a Privacy Impact Assessment or PIA—is a crucial first step in successful P/CRCL policy development. A PIA allows leaders of an information sharing initiative to analyze privacy risks and exposures of data stored and exchanged by organizations participating in multijurisdictional information collaborations. Resulting policies specifically address these risks.

**Terms and Definitions**

**Personally Identifiable Information—** Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

**Privacy Impact Assessment (PIA)—**A process by which an entity can examine the P/CRCL risks in the justice entity's information system and sharing activities. In general, a PIA evaluates the process through which PII is collected, stored, protected, shared, managed, and purged. By completing a PIA, entities are able to identify P/CRCL vulnerabilities and to address and mitigate them through the design and implementation of policies.

**Privacy, Civil Rights, and Civil Liberties (P/CRCL) Policy—**A printed, published statement that articulates the policy position of an entity on how it handles the PII that it maintains and uses in the normal course of business. The policy should include information relating to the processes of information collection, receipt, access, use, dissemination, retention, and purging. It is likely to be informed by the Fair Information Practice Principles (FIPPs). The purpose of the P/CRCL policy is to articulate that the entity will adhere to those legal requirements and center policy determinations that enable collection, receipt, access, use, dissemination, retention, and purging of information to occur in a manner that protects personal privacy interests. A well-developed and implemented P/CRCL policy uses justice entity resources wisely and effectively; protects the entity, the individual, and the public; and promotes public trust.

## III. What Is Contained Within This Guide?

This guide provides the following:

- A PIA overview.
- A PIA template that leads practitioners through appropriate privacy risk assessment questions. The template is provided as Appendix A.
- A glossary of relevant terms and definitions in Appendix B.
- Two methods to institutionalize the PIA process for information systems development: model legislation and a draft governor's executive order. Model legislation is provided as Appendix C, and the draft executive order as Appendix D.
- OMB guidance for implementing the E-Government Act of 2002 in Appendix E.
- Information and Resources about Social Media in Appendix F.
- An explanation of the Fair Information Practice Principles in Appendix G.

[1] Office of Management and Budget Memorandum (OMB M-03-022), *OMB Guidance for Implementing the Privacy Provision of the E-Government Act of 2002*, contained in Appendix E.

# PIA Overview

## I. What Is a PIA?


**A Privacy Impact Assessment—**a process by which an entity can examine the P/CRCL risks in the justice entity's information system and sharing activities. In general, a PIA evaluates the process through which PII is collected, stored, protected, shared, managed, and purged. By completing PIAs, entities can identify P/CRCL vulnerabilities and address and mitigate them through the design and implementation of policies.

Taking a cue from the federal E-Government Act, which requires PIAs for new or significantly modified federal IT systems, a PIA supports the notion that before diving into full P/CRCL policy development, state, local, tribal, and territorial jurisdictions should first identify, analyze, and assess the risks associated with information systems that are used to secure the privacy of the data and information they store and share. Once risks are identified and analyzed, policies can specifically address and mitigate the risks.

A PIA evaluates privacy implications when information systems are created or when existing systems are significantly modified. PIAs can also be conducted for existing IT systems that fall into neither of these two categories. Routine PIA use is a cost-effective demonstration of sound public policy. For more information, a variety of state, local, tribal, and territorial (SLTT) and federal PIA resources are available at https://it.ojp.gov/privacy/.

## II. The PIA Process

The following briefly highlights the PIA process.

- The PIA process begins with the completion of a Privacy Threshold Analysis (PTA) to determine which systems need a PIA. This analysis will identify information that will be exchanged, with whom it will be exchanged, and whether there are any associated privacy, civil rights, or civil liberties implications.
- Next, the PIA poses a series of questions that help stakeholders identify and understand any risks their systems may pose to the privacy, civil rights, and civil liberties of personally identifiable information.
- Privacy policies emerge as the result of the identification and analysis that occur during the PIA process, generating discussion and decision making on how to address and mitigate, if necessary, the identified privacy vulnerabilities.

## III. Why Is a PIA Important?

Protecting information privacy, civil rights, and civil liberties is a foundational concept. Information systems used by law enforcement and other justice entities are perhaps more closely scrutinized than other government or privately operated information systems; therefore, they are held to higher standards.

Higher standards are expected for information that can deprive individuals of their personal freedom or that can put individuals such as victims and witnesses at risk. In addition, criminal justice data is often collected without the consent of a data subject, who may be an alleged offender, a crime victim, or a witness. Greater diligence in handling personally identifiable information is crucial for safeguarding the interests of individuals who have little or no choice about becoming involved in the criminal justice system.

Essential to American democracy is the ability to hold government accountable for its actions through a variety of state and federal transparency laws that allow citizens to gain access to public meetings and official records.

Conducting a PIA illustrates an SLTT entity's commitment to and thoughtful analysis of protection of the public's information. Maintaining public trust is at the core of the PIA concept; this is particularly true for criminal justice entities. The public must be assured that personally identifiable information and confidential data will be gathered and used in an authorized and lawful manner. There are many practical and philosophical reasons to conduct a PIA. Addressing privacy concerns early in the design process can encourage policymaker support, as well as financial support, for a system. An effective PIA process may not gain public support for a particular program or initiative but is likely to stimulate healthy debate and deflate potential opposition to important information sharing capabilities.

Failing to recognize privacy values can result in system shutdown, forced data destruction, costly modifications, implementation delays, and more restrictive legislative mandates, as well as personal and agency embarrassment.

Primarily, however, a PIA should be conducted to ensure that personally identifiable information and confidential information entrusted to an agency is appropriately protected in accordance with the sensitivity of the information, sparing record subjects—whose interaction with the justice system is already almost assuredly causing tension—further trauma or even victimization by the improper use and exchange of their data.

**State PIA Example—Ohio**

**Privacy Impact Statements and Assessments**

**In Ohio, commitment to the detection of privacy risks and assurance of privacy protections for the personally identifiable information (PII) state agencies handle is demonstrated by Ohio state law, as follows:**

**"To ensure privacy is considered, state agencies are required to create privacy impact statements in accordance with Section 125.18 [C][2] of the Ohio Revised Code (ORC) . . . a Privacy Impact Assessment (PIA) is [considered] the same as a privacy impact statement. Section 1347.15[B][8] of the Ohio Revised Code also requires state agencies to complete privacy impact assessment forms. [In addition,] each state agency is required to have a Data Privacy Point of Contact (DPPOC) to assist the agency's program unit in completing a PIA.**

**Furthermore, performing a PIA upon the collection of new types of information or at the beginning of the development or acquisition of a new information system that maintains PII will help a state agency to determine most, if not all, of the necessary privacy and security controls."**

**This PIA process penetrates agencies statewide, such as the Ohio Department of Public Safety and many others that handle confidential personal information. Ohio even goes one step farther by performing compliance checks administered by the Ohio state auditor.**

**Ohio.gov, Privacy and Security website, at https://infosec.ohio.gov/Portals/0/Docs/Ohio_PIA_2013.pdf.**

## IV. When to Perform a PIA

As mentioned earlier, a PIA can be conducted to evaluate privacy implications when information systems are created, when existing systems are significantly modified, and at any other time. In general, PIAs should be performed and updated as necessary where a system change creates new privacy, civil rights, and civil liberties risks. Appendix E provides a detailed list of these conditions, as recommended by the Office of Management and Budget, and the Fair Information Practice Principles (FIPPs) in Appendix G provide the analytic framework for process.

You should first conduct two fundamental analyses to determine whether your system needs a PIA:

- First, analyze your system and information sharing initiative itself by asking this simple question**:** "Which systems might need a PIA?" See A. for more information.
- Then, conduct a privacy threshold analysis (PTA) to determine whether your system collects personally identifiable information (PII). See B. for more information.

## A. Which Systems Need a PIA?

Examine your information system(s) and the information sharing initiative itself. The question is, Which systems need a PIA? The answers are easy: generally, any new data system—especially any new information sharing initiative—that collects PII should be subjected to a PIA as part of the planning process. In addition, any significant modification of an existing system should be the subject of a PIA if the modifications are associated with the collection, use, access, or dissemination of PII.

Therefore, determining whether your systems collect personally identifiable information—information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual[2]—is the second analytical step.

## B. Privacy Threshold Analysis

If in doubt as to whether a PIA is appropriate, performing a PTA will help ascertain whether a PIA is needed for system upgrades or improvements. The first question is, Does the system store, use, or otherwise maintain personally identifiable information? If your answer is yes, consider the following:

**Privacy Threshold Question 1: What information about individuals could be collected, generated, or retained?**

***Rationale.*** Creating a list of the types of PII a system will use stored requires that designers appropriately consider the types of PII data their systems will collect. Obvious types are name, address, and social security number. Less obvious types are information that can be linked or that is linkable to specific individuals. Note that information about individuals can even include their images captured by cameras monitoring specific locations or information about health status that may be detected by a system designed to capture radioactivity levels and thus determine whether an individual received chemotherapy. Privacy can be threatened when seemingly innocuous pieces of personally identifiable information—such as individual preferences that facilitate a website's use or proof of age on driver's licenses shown for participation in a separate age-restricted activity—are "bundled" in a single record. Privacy can also be endangered by the use of global positioning devices, cell phones, personal digital assistants, surveillance cameras, radio frequency identification tags, home wireless networks, and other technologies that could be monitored to provide information on where a person lives or works.

**Privacy Threshold Question 2: Does your system operate under specific or general legal authority?**

***Rationale.*** Many agencies operate systems under their general statutory or other legal operating authority.[3] Some operate under specific legislation or regulation applicable to their information systems. You must determine whether either of these two conditions exists and ensure that your assessment and resulting P/CRCL policy comply with the provisions of any such laws or regulations. Be aware, however, that some statutes might not adequately address the privacy protections that should be provided to the information collected. If no such specific regulations exist in your jurisdiction or the statute or regulation does not adequately address privacy, at minimum you should align your

[2] For further information about the breadth of PII and how to perform an assessment of the specific risk that an individual can be identified using the information, see Revision of Office of Management and Budget Circular A-130: Managing Information as a Strategic Resource, July 2016, https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.

[3] Where applicable, you should consider what impact tribal privacy laws may have with regard to information collected, generated, maintained, or distributed by tribal government agencies. Tribal users may also want to consult the Indian Civil Rights Act of 1968, United States Code, Title 25, Chapter 15, Subchapter I, § 1301.

P/CRCL policy with the best practices as enumerated in the various existing state and federal laws, such as the Federal Privacy Act[4] and the Code of Federal Regulations.

**Privacy Threshold Question 3: Has a PIA ever been conducted on your information system?**

*Rationale.* PIAs are generally conducted at the beginning of an information system's design phase or when a system undergoes a significant upgrade. However, if your system collects, maintains, or generates PII, it would be wise to conduct a PIA even if your system does not fall into these two categories. A PIA will identify the privacy implications and the characteristics of your IT system and will inform your assessment of how your entity may mitigate privacy vulnerabilities before a breach occurs. Your answers to these questions will reveal the P/CRCL policy needs of your system and will help you to decide whether to conduct a PIA.

## V. Steps to Developing the P/CRCL Policy: Where the PIA Fits In

### Step 1 Systems and Privacy Threshold Analyses (PTA).

Analyze the information system and information use, maintenance, and sharing to determine which systems need a PIA. Then, conduct a PTA for each system. Take these additional steps after determining your system or information sharing initiative's P/CRCL policy needs:

### Step 2 Identify and analyze your shared information.

It is important to articulate the information exchanges that will occur in your system to understand how information will be shared across the system and with participating organizations. Knowing the agencies and organizations involved, what data they will share, when and under what circumstances it will be shared, and what the information will be used for is critical in understanding any privacy implications. It helps to follow a consistent, intuitive approach to capturing information-exchange requirements. For example, for each exchange, identify who is involved (what agencies/organizations), what the legal authorities are for the exchange, why the exchange is taking place (specifying the distinct mission, business, or operational needs for the process), when it takes place (mission, business, or operational events and conditions), and what information is being exchanged. This analysis can be useful in understanding potential privacy risks, as well as in specifying privacy rules within a P/CRCL policy. For more information on resources available to assist entities in analyzing information exchanges, refer to the Global P/CRCL Policy Guide, Section 7. Understanding Information Exchanges.[5]

### Step 3 Conduct the PIA. (Use the template contained in Appendix A.)

### Step 4 Develop your privacy, civil rights, and civil liberties policies.

Use the Global P/CRCL Policy Guide and the SLTT Policy Development Template, referenced earlier, to develop the content of your entity's privacy, civil rights, and civil liberties policy.[6]

## VI. Should You Publicize the Completed PIA?

A completed PIA can be a valuable public relations tool to proactively address privacy and other identified concerns as a system nears implementation. Prominent posting of a completed PIA on a website or at an agency's office promotes transparency and fosters public trust. Posting the PIA or otherwise making it publicly available enables the public and policymakers to evaluate its thoroughness and accuracy. The

[4] Privacy Act of 1974, 5 U.S.C. § 552a, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a.
[5] Refer to the Global P/CRCL resources available at www.it.ojp.gov/privacy.
[6] Ibid.

PIA also demonstrates an agency's role as a trusted data steward. An agency may also consider other methods, such as press releases, to increase public awareness of its completed PIA.

## VII. Who Conducts the PIA?

Fundamental to information sharing system development are (1) agreement on guiding principles and (2) identification of strategic and tactical issues. Conducting a PIA during the strategic planning process ensures that privacy issues are addressed early and are incorporated into the system design and governance. Ideally, a PIA is completed by information system stakeholders (the governance group) as part of a strategic planning process and in collaboration with the agency's legal counsel, record managers, those responsible for data privacy, those responsible for freedom of information responses, and system security personnel.

The completed PIA is then submitted to the information system's governing/decision-making body. PIA results will show decision makers which policies are needed or identify any other work that might be necessary. In smaller organizations or information systems efforts, PIA responsibilities may belong to an individual rather than to a group; nevertheless, smaller agencies may still wish to involve multidisciplinary stakeholders and other individuals from outside their agencies to assist in PIA preparation. They can identify privacy issues and suggest ways to mitigate the associated risks. Interested and/or affected parties to supplement internal agency resources could include the following:

- Privacy, civil rights, and civil liberties advocates
- Private/public records managers
- Civil liberties organizations
- Advisory or oversight members
- Elected officials
- Legislative research staff
- IT associations
- Other justice IT professionals
- Prosecutors
- Public defenders
- Judges
- Corrections, probation, and parole professionals

**A Note About Resources**

**The authors of this guide acknowledge that the PIA process may initially seem too complex or time-intensive for rural agencies and smaller departments that may have limited resources to devote to this task. It is important to remember that, in order to adequately analyze agency privacy risks, each question in the template contained in Appendix A will need to be addressed and answered. One way for smaller agencies to do this may be to pool resources for the purpose of completing the PIA. Bringing together individuals from a number of small agencies, each of whom, according to his or her respective position and responsibilities, utilizes the information system being assessed, will be helpful in completing the PIA process when none of the agencies has the resources to conduct a comprehensive PIA on its own. If appropriate, the entity also may consider reaching out to local professional associations (for law enforcement, for example, this may be sheriffs' or police chiefs' associations) or other organizations for assistance.**

In addition, there may be other groups, such as public safety-minded local businesses, that could provide technical resources. A local hospital or medical provider may have a Health Insurance Portability and Accountability (HIPAA) expert whose knowledge in protecting health information could be useful in assessing your system's privacy implications. If no local civil liberties groups or public defenders are available, nonprofit organizations with outreach efforts around social justice issues, such as local churches and faith communities, could assist. In addition to gaining valuable expertise, allowing stakeholders to participate in the PIA preparation process demonstrates an agency's commitment to inclusiveness and openness. Ultimately, the PIA process should be as inclusive as possible to address the perspectives of members of the public who may be affected by the system. Including stakeholders in your review process gives you an opportunity to address their privacy concerns and may even eliminate some.

Ultimately, it is the responsibility of the governing body in a multiorganizational effort or of the agency executive in a smaller initiative to address the potential risks revealed by the PIA. These leaders will then

determine whether the risks are acceptable, can be mitigated via policy or process development, or could result in a decision not to move forward with the project.

## VIII. PIA Components

At minimum, a PIA should analyze and describe:

- What personally identifiable information is to be collected (e.g., nature and source).
- Why information is being collected (e.g., to determine eligibility).
- How the PII will be collected and used (e.g., to verify existing data).
- How and by whom the PII will be accessed and with whom the PII will be shared (e.g., another agency for a specified programmatic purpose).
- How the PII will be stored.
- What opportunities individuals will have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses) and how individuals can grant consent. (Note: This is of particular importance, since collection of criminal justice data is often not voluntary or provided with consent.)
- How the PII will be secured.

## IX. PIA Outcome

A completed PIA should:

- Identify privacy, civil rights, and civil liberties vulnerabilities and risks for stakeholders, owners, entity heads, and others accountable for a system's operation.
- Include a summary of mitigating actions to address identified privacy risks. Ideally, the individual completing the PIA should have the authority to direct mitigation steps, not just to recommend changes after the fact. A PIA that identifies the potential risks and describes what steps may be taken to mitigate the risks reflects poor privacy protection planning and is nothing more than an expression of a hope to improve in the future. In contrast, a PIA that explains how potential privacy risks were mitigated via system design or other protections demonstrates that privacy was built into the system and was not just a theoretical goal.
- Most important, identify which privacy, civil rights, and civil liberties protection policies must be developed to mitigate or eliminate potential risks to data maintained in the system.

Stakeholders can share the PIA to engage the public, policymakers, and others in a dialogue about the system, thereby fostering greater public trust. Policies that result from the PIA can include:

- Enhanced security features, such as improved audit capability or enhanced physical security.
- An updated records retention schedule.
- Publication of the purpose statement and P/CRCL policy on the agency website or in a state register.
- Audit procedures.
- Challenge processes for data that originates in other systems.

The PIA will ultimately serve as the first step in identifying the privacy implications and vulnerabilities of your information system. It is a road map for developing a thoughtful and comprehensive P/CRCL policy to protect personally identifiable information and confidential information and will serve the needs of your agency and the public.

## X. Institutionalizing the PIA Process

Conducting a PIA at the state, local, tribal, and territorial levels is a best practice that should become a standard component of any strategic planning process aimed at automation and information sharing. As noted previously, the E-Government Act of 2002 requires federal agencies to conduct PIAs of new or significantly modified information systems. Few states have statutory requirements to conduct PIAs, either of new, significantly modified, or existing information systems. If your state is considering institutionalizing a PIA process, model legislation in Appendix C and a governor's executive order in Appendix D provide suggestions for such undertakings.

**Federal PIA Example—DHS Conducts PIA, Results in Notice and Redress**

**The U.S. Department of Homeland Security (DHS), Customs and Border Protection (CBP) conducted a PIA of its Automated Commercial Environment (ACE) System, a program to monitor passage of commodities, materials, crew members, and passengers across U.S. borders.**

**As a result of the PIA process, participating truck carriers are asked to provide their drivers with notice regarding the collection and use of their information as well as how to seek redress if their records are inaccurate. CBP created a fact sheet to provide drivers with additional notice.**

**See https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_aceitds.pdf.**

### A. Social Media

State, local, tribal, and territorial entities are turning to social media sites both as a communications tool and as an open source of information to support law enforcement investigative activities. Conducting a PIA on the organization's process, procedures, and intended use of publicly available information (including social media) helps the public understand the entity's authorities and process; determines, for law enforcement and the entity as a whole, where the privacy risks exist; and provides useful insights into the planning around the organization's presence on social media. Appendix F outlines resources, including guidance from federal agencies, the Global Justice Information Sharing Initiative, and the International Association of Chiefs of Police (IACP) Center for Social Media, to assist in the use of PIAs for an entity's social media process.

# Conclusion

As outlined in this guide, the consequences of inadequate or careless data protections are too severe for SLTT justice entities to delay assessing the privacy implications and vulnerabilities of their information systems. News stories about agencies that failed to properly protect their data and that permitted personally identifiable information and confidential information to fall into the wrong hands are all too common. Do not let your entity make the headlines for the wrong reasons; perform a PIA to identify possible privacy risks associated with the entity's information sharing system.

## Where to Turn for More Information

Once the PIA is complete, entities are encouraged to refer to resources for Stage 3—"Develop the P/CRCL policy" in the Privacy Program Cycle for tools to assist in the policy development process. For more information on all of the privacy resources available for each stage of a Privacy Program Cycle, refer to DOJ's *Global Privacy Resources*, available at www.it.ojp.gov/privacy.

For more information on the development of this and other Global privacy resources, as well as to request printed copies, please send a request via email to GLOBAL@iir.com.

# Appendix A—Privacy Impact Assessment Template

**Instructions for Completing the Privacy Impact Assessment—PIA Template Column Headings**

The following information is provided to assist individuals in performing a PIA.

**Template Section—**PIA questions are grouped into sections of related policy concepts that mirror the framework of the *Privacy, Civil Rights, and Civil Liberties Policy Development Template for State, Local, Tribal, and Territorial Justice Entities* (SLTT Policy Development Template), used to draft the entity P/CRCL policy. Structuring the questions in this format prepares the practitioner performing the PIA for the next step, applying this information to the P/CRCL policy.

**PIA Questions—**Pose questions for response or action.

**Suggested Respondent(s)—A** general list of individuals (or roles) within the entity who are recommended to answer or contribute to the answer to a particular question. Other appropriate positions may be added or substituted as needed.

**Entity Administrator:** The chief executive officer or chief operations officer of the agency or organization. This could also be a department or division head over the organizational unit responsible for data collected and shared via an information exchange.

**System Administrator:** The chief information officer or other senior official responsible for overseeing the overall IT functions of an agency or organization.

**Privacy and Civil Liberties Officer/Legal Counsel:** The agency or organization privacy officer or attorney responsible for ensuring that the entity complies with all relevant privacy laws and policies. This should be the person who acts as the senior policy advisor on overall P/CRCL policy, including legislative language, regulations, and other nonregulatory guidance related to or including privacy, confidentiality, or data security.

**Technical/Systems Security Staff:** The agency or organization staff person(s) responsible for implementing the technical enforcement of all relevant privacy and security policies (e.g., user authentication, access control, audit logs, firewalls, encryption).

**Answer—**The respondent(s) respond(s) to each question, as appropriate:

**Yes** – Fully meets requirement

**No** – Does not meet requirement

**Incomplete** – Partially meets requirement

**N/A** – Does not apply

**Assessment of Risk—**Make a judgment as to the likelihood, severity, and risk tolerance level of the privacy risk.[7] Recommended guidelines:

**Likelihood that risk will occur**

**Remote:** The risk probably will not occur because the risk would be difficult to realize, or there are solid means in place to limit the risk appropriately.

**Possible:** The risk has a chance of occurring, but it may be difficult or there are policies or procedures in place to help avoid the risk.

**Likely:** Because of conditions and capabilities, the risk is likely to occur.

**Severity of identified risk**

**Low:** The risk is manageable through planning and action, and the impacts generally are minimal.

**Medium:** The risk will be mitigated through planning and action. If it occurs, it will still have some impact on more important areas of concern.

**High:** The risk will have serious impacts; without extensive planning and action, its consequences would be severe.

**Your tolerance for that risk**

**Avoidance:** Avoidance is often used for risks that have the capacity for negative impact but have little known recourse. In privacy projects, a decision to avoid risks often means a decision not to let your agency put itself in a situation wherein it could incur the risk. Therefore, your decision would also be to avoid the cause of the risk.

**Assume:** The decision to assume a risk means accepting the risk as is and not implementing any policies or procedures to lessen it. This is often the decision in cases where the risk is so minimal and of such limited impact, should it occur, that the cost of implementing a mechanism to minimize or reduce it would be far greater than the agency's concern.

**Mitigate:** This is the most common decision to make for identified risks: to implement policies, procedures, and other controls to limit the risk to an acceptable level.

**Transfer:** Transfer the responsibility for a system or the risk itself to another party that can better accept and deal with the risk and/or that has the resources necessary to properly mitigate the risk.

- In the Corrective Action/Remediation column, record the corrective action or recommendation that your initiative will take to mitigate the identified risk.
- In the Assessment of Risk column, record the priority level of the risk: either 1 (high priority), 2 (moderate priority), or 3 (lowest priority).

[7] For more about risk assessment, see *Law Enforcement Tech Guide for Information Technology Security: How to Assess Risk and Establish Effective Policies*, prepared by SEARCH, The National Consortium for Justice Information and Statistics, and published by the Office of Community Oriented Policing Services, U.S. Department of Justice. Available at www.search.org/files/pdf/ITSecTechGuide.pdf.

**Corrective Action/Remediation/Location—**If the answer to the PIA question is "No" or "Incomplete," then respond in the Corrective Action/Remediation column as to what steps will be taken to respond to this requirement and who will be responsible for taking the necessary action(s).

If the answer to the PIA question is "Yes," then respond in the Corrective Action/Remediation column as to where the necessary information can be located to be included or referenced in the entity's privacy, civil rights, and civil liberties policy.

**This page intentionally left blank.**

# PIA Cover Page

| | |
|---|---|
| **Information Sharing System or Exchange(s) Assessed:** | |
| **System Names:** | |
| **Purpose:** | |
| **Assessment Date(s):** | |
| **Organizations/Entities Involved:** | **Assessors (Entity Representatives):** |
| | |
| | |
| | |
| | |
| | |
| **Project Manager:** | |
| **Final PIA Submitted to:** | |
| **Date Submitted:** | |
| **Approved by:** | |
| **Approval Date:** | |

**This page intentionally left blank.**

# Privacy Impact Assessment

| Template Section | PIA Questions | Suggested Respondent(s) | Answer (Yes, No, Incomplete, or N/A) | Assessment of Risk | Corrective Action/ Remediation/ Location |
|---|---|---|---|---|---|
| **A. Purpose Specification** | 1. Is there a written mission statement for the entity? | Entity Administrator | | | |
| | 2. Is there a written purpose statement for collecting personally identifiable information (PII)? Include all types. | Entity Administrator Privacy and Civil Liberties Officer/Legal Counsel | | | |
| | 3. Does the entity's mission statement support the purpose for collecting PII? | Entity Administrator Privacy and Civil Liberties Officer/Legal Counsel | | | |
| **B. Policy Applicability and Legal Compliance** | 1. Does the entity have legal authority for collecting, creating, storing, accessing, receiving, and sharing or viewing data? If so, include citation(s), if applicable. | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |
| | 2. Will all individuals with physical or logical access to the entity information be subject to the privacy, civil rights, and civil liberties (P/CRCL) policy? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |

| Template Section | PIA Questions | Suggested Respondent(s) | Answer (Yes, No, Incomplete, or N/A) | Assessment of Risk | Corrective Action/ Remediation/ Location |
|---|---|---|---|---|---|
| | 3. How does the entity plan to provide the P/CRCL policy to personnel, participating users, and individual users (for example, in print, online)? | System Administrator | | | |
| | 4. Will the entity require all individuals with physical or logical access to acknowledge receipt of the policy and agree to comply with the policy (in writing or online)? | System Administrator | | | |
| | 5. Will the entity require that individuals with physical or logical access and information-originating and user agencies be in compliance with all applicable constitutional and statutory laws protecting privacy, civil rights, and civil liberties in the gathering and collection, use, analysis, retention, destruction, sharing, disclosure, and dissemination of information?<br><br>Note: These laws, statutes, and regulations will be cited in the P/CRCL policy. | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |

| Template Section | PIA Questions | Suggested Respondent(s) | Answer (Yes, No, Incomplete, or N/A) | Assessment of Risk | Corrective Action/ Remediation/ Location |
|---|---|---|---|---|---|
| | 6. Is a privacy notice required by law before data is collected, where appropriate (usually limited to health records)? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |
| **C. Governance and Oversight** | 1. Is primary responsibility for the entity's overall operation—including the information systems, information collection and retention procedures, coordination of personnel, and enforcement of the P/CRCL policy—assigned to one or more individuals? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |
| | 2. Will the entity have a privacy oversight committee or team that is responsible for the development of the privacy policy and/or that will routinely review and update the policy? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |
| | 3. Will the entity designate and train a privacy officer to handle reported errors and violations and oversee the implementation of privacy protections? | System Administrator | | | |

| Template Section | PIA Questions | Suggested Respondent(s) | Answer (Yes, No, Incomplete, or N/A) | Assessment of Risk | Corrective Action/ Remediation/ Location |
|---|---|---|---|---|---|
| | 4. Will the entity assign responsibility for ensuring that enforcement procedures and sanctions for noncompliance with the P/CRCL policy are adequate and enforced? | Entity Administrator | | | |
| **D. Definitions** | 1. Has the entity defined the primary terms that will be used in the policy for which the entity wants to specify particular meanings? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |
| **E. Information** | 1. Has the entity identified the information it will seek, collect, retain, share, disclose, or disseminate? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |
| | 2. Has the entity identified what information may not be sought, retained, shared, or disclosed by the entity? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |
| | 3. Does the entity apply labels to information based on legal or policy restrictions or information sensitivity to indicate to authorized users how to handle the information? | Entity Administrator OR Privacy and Civil Liberties Officer/Legal Counsel OR Technical/Systems Security Staff | | | |

| Template Section | PIA Questions | Suggested Respondent(s) | Answer (Yes, No, Incomplete, or N/A) | Assessment of Risk | Corrective Action/ Remediation/ Location |
|---|---|---|---|---|---|
| | 4. Does the entity categorize information based on its type (for example, tips and leads, suspicious activity reports, criminal history, intelligence information, case records, conditions of supervision, case progress), usability, and quality? | Entity Administrator OR Privacy and Civil Liberties Officer/Legal Counsel OR Technical/Systems Security Staff | | | |
| | 5. Does the entity require certain basic descriptive information to be associated with each record, data set, or system of records containing PII (for example, source, originating entity, collection date, and contact information)? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel OR Technical/Systems Security Staff | | | |
| | 6. Is personally identifiable information obtained with the knowledge or consent of the data subject, if appropriate? | System Administrator | | | |

| Template Section | PIA Questions | Suggested Respondent(s) | Answer (Yes, No, Incomplete, or N/A) | Assessment of Risk | Corrective Action/ Remediation/ Location |
|---|---|---|---|---|---|
| **F. Acquiring and Receiving Information** | 1. Are there applicable state and federal constitutional provisions and statutes that govern or specify the techniques and methods the entity may employ when seeking and receiving information?<br><br>Note: These laws, statutes, and regulations will be cited in the P/CRCL policy. | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |
| | 2. Does the entity's SAR process provide for human review and vetting to ensure that information is both gathered in an authorized and lawful manner and, when applicable, determined to have a potential terrorism nexus? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |

| Template Section | PIA Questions | Suggested Respondent(s) | Answer (Yes, No, Incomplete, or N/A) | Assessment of Risk | Corrective Action/ Remediation/ Location |
|---|---|---|---|---|---|
| | 3. Has the entity established a SAR process that includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved in activities that have been determined to be consistent with criminal activities associated with terrorism will be documented and shared through the ISE? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |
| | 4. Does the entity require law enforcement officers and appropriate entity and participating entity staff members to be trained to recognize the behaviors and incidents that are indicative of criminal activity associated with terrorism? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |
| | 5. Does the entity (if operational, conducting investigations) adhere to a policy regarding the investigative techniques to be followed when acquiring information (for example, an intrusion-level statement)? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |

| Template Section | PIA Questions | Suggested Respondent(s) | Answer (Yes, No, Incomplete, or N/A) | Assessment of Risk | Corrective Action/ Remediation/ Location |
|---|---|---|---|---|---|
| | 6. Do agencies that access your entity's information and/or share information with your entity ensure that they will adhere to applicable law and policy? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |
| | 7. Does the entity contract with commercial databases and, if so, does the entity ensure that the commercial database entity is in legal compliance in its information-gathering techniques? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |
| **G. Data Quality Assurance** | 1. Has the entity established procedures and processes to ensure the quality (for example, accurate, complete, current, verifiable, and reliable) of the information it collects and maintains, including procedures for responding to alleged or suspected errors or deficiencies (for example, correction or destruction)? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |

| Template Section | PIA Questions | Suggested Respondent(s) | Answer (Yes, No, Incomplete, or N/A) | Assessment of Risk | Corrective Action/ Remediation/ Location |
|---|---|---|---|---|---|
| | 2. Does the entity apply labels (or ensure that the originating agency has applied labels) to the information regarding its level of quality (for example, accurate, complete, current, verifiable, and reliable)? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel OR Technical/Systems Security Staff | | | |
| | 3. Does the entity review the quality of the information it originates to identify data that may be inaccurate or incomplete? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |
| | 4. When information that is received from or provided to another agency is determined to be inaccurate or incomplete, does the entity notify the originating or recipient agency? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |
| **H. Collation and Analysis** | 1. Is there a policy stating the purpose for which information is analyzed and specifying who is authorized (position/title, credentials, etc.) to analyze information? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |

| Template Section | PIA Questions | Suggested Respondent(s) | Answer (Yes, No, Incomplete, or N/A) | Assessment of Risk | Corrective Action/ Remediation/ Location |
|---|---|---|---|---|---|
| | 2. Has the entity defined what information can be analyzed? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |
| **I. Merging Records** | 1. Does the entity identify who is authorized (position/title, credentials, clearance level[s], etc.) to merge records? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel OR Technical/Systems Security Staff | | | |
| | 2. Does the entity define matching criteria for merging information from multiple records allegedly about the same individual (e.g., sufficient identifying information beyond "name")? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel OR Technical/Systems Security Staff | | | |
| | 3. If the criteria specified above are not met, does the entity have a procedure for partial matches?<br><br>Note: If the agency or exchange does not merge records that have partial matches, the policy should state this. | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel OR Technical/Systems Security Staff | | | |

| Template Section | PIA Questions | Suggested Respondent(s) | Answer (Yes, No, Incomplete, or N/A) | Assessment of Risk | Corrective Action/ Remediation/ Location |
|---|---|---|---|---|---|
| **J. Sharing and Disclosure** | 1. Does the entity assign credentialed role-based levels of access for authorized users (for example, class of access and permissions to view, add, change, delete, or print)? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel OR Technical/Systems Security Staff | | | |
| | 2. Has the entity defined the conditions and credentials for access to and disclosure of records within the entity or in other governmental entities (for example, for law enforcement, public protection, public prosecution, public health, or justice purposes)? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel OR Technical/Systems Security Staff | | | |
| | 3. Are participating agencies that access information from your entity required to obtain approval from the originator of the information prior to further dissemination or to follow the disclosure laws applicable to the originating agency? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |

| Template Section | PIA Questions | Suggested Respondent(s) | Answer (Yes, No, Incomplete, or N/A) | Assessment of Risk | Corrective Action/ Remediation/ Location |
|---|---|---|---|---|---|
| | 4. Has the entity identified those laws or policies that specify when a record can be disclosed to a member of the public? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |
| | 5. Does the entity maintain an audit trail to document access to and disclosure of information retained by the entity (e.g., dissemination logs)? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel OR Technical/Systems Security Staff | | | |
| | 6. If release of information can be made only under exigent circumstances, are those circumstances described? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |
| | 7. Does the entity adhere to laws or policies for confirming the existence or nonexistence of information to persons or agencies that are not eligible to receive the information? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |

| Template Section | PIA Questions | Suggested Respondent(s) | Answer (Yes, No, Incomplete, or N/A) | Assessment of Risk | Corrective Action/ Remediation/ Location |
|---|---|---|---|---|---|
| **K. Redress**<br><br>**K.1 Disclosure** | **Disclosure**<br>1. If required by law or policy, has the entity established procedures for disclosing information to an individual about whom information has been gathered (for example, proof of identity, fingerprints)? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |
| | 2. Are there conditions under which an entity will not disclose information to an individual about whom information has been gathered?<br><br>Note: The P/CRCL policy will cite applicable legal authority for each stated basis for denial. | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |
| | 3. If the entity did not originate and does not have the right to disclose it, are there circumstances in which the entity will either refer the individual to the agency originating the information or notify the originating agency of the request? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |

| Template Section | PIA Questions | Suggested Respondent(s) | Answer (Yes, No, Incomplete, or N/A) | Assessment of Risk | Corrective Action/ Remediation/ Location |
|---|---|---|---|---|---|
| **K.2. Corrections** | **Corrections**<br>1. Has the entity established procedures for handling individuals' requests for correction involving information the entity has disclosed and can change because it originated the information? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |
| **K.3 Appeals** | **Appeals**<br>1. If requests for disclosure or corrections are denied, does the entity have established procedures for appeal? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |
| **L. Security Safeguards** | 1. Does the agency or exchange have a designated security officer? | Entity Administrator OR Privacy and Civil Liberties Officer/Legal Counsel OR Technical/Systems Security Staff | | | |

| Template Section | PIA Questions | Suggested Respondent(s) | Answer (Yes, No, Incomplete, or N/A) | Assessment of Risk | Corrective Action/ Remediation/ Location |
|---|---|---|---|---|---|
| | 2. Does the entity have physical, procedural, and technical safeguards for ensuring the security of its data?<br><br>Note: The P/CRCL policy will describe how information will be protected from unauthorized access, modification, theft, or sabotage (whether internal or external) resulting from natural or human-caused disasters or intrusions with, for example, procedures, practices, system protocols, use of software, information technology tools, and physical security measures. | Entity Administrator OR Privacy and Civil Liberties Officer/Legal Counsel OR Technical/Systems Security Staff | | | |
| | 3. Is information stored in a secure format and a secure environment? | Entity Administrator OR Privacy and Civil Liberties Officer/Legal Counsel OR Technical/Systems Security Staff | | | |
| | 4. Does the entity utilize watch logs to maintain audit trails of requested and disseminated information, and do logs identify the user initiating the query? | Entity Administrator OR Privacy and Civil Liberties Officer/Legal Counsel OR Technical/Systems Security Staff | | | |

| Template Section | PIA Questions | Suggested Respondent(s) | Answer (Yes, No, Incomplete, or N/A) | Assessment of Risk | Corrective Action/ Remediation/ Location |
|---|---|---|---|---|---|
| | 5. Will all personnel who are subject to the P/CRCL policy be required to report suspected or confirmed breaches? | Entity Administrator OR Privacy and Civil Liberties Officer/Legal Counsel OR Technical/Systems Security Staff | | | |
| | 6. Does the entity have established procedures for adhering to data breach notification laws or policies? | Entity Administrator OR Privacy and Civil Liberties Officer/Legal Counsel OR Technical/Systems Security Staff | | | |
| **M. Information Retention and Destruction** | 1. Does the entity have a records retention and destruction policy (including methods for removing or destroying information)? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |
| | 2. Does the entity have a review schedule for validating or purging information? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |
| | 3. Will there be a periodic review of collected data to make sure they are still needed? If so, include the review schedule. | System Administrator | | | |

| Template Section | PIA Questions | Suggested Respondent(s) | Answer (Yes, No, Incomplete, or N/A) | Assessment of Risk | Corrective Action/ Remediation/ Location |
|---|---|---|---|---|---|
| **N. Accountability and Enforcement**<br><br>**N.1 Information System Transparency** | **Information System Transparency**<br>1. Will the P/CRCL policy be available on the entity's public website? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |
| | 2. Does the entity have a point of contact (position/title) for handling inquiries or complaints? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |
| **N.2 Accountability** | **Accountability**<br>1. Are there procedures and practices the entity follows to enable evaluation of user compliance with system requirements and applicable law, as well as its P/CRCL policy, when established? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel OR Technical/Systems Security Staff | | | |
| | 2. Is there an established mechanism for personnel to report errors and suspected or confirmed violations of policies related to protected information? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |

| Template Section | PIA Questions | Suggested Respondent(s) | Answer (Yes, No, Incomplete, or N/A) | Assessment of Risk | Corrective Action/ Remediation/ Location |
|---|---|---|---|---|---|
| **N.3 Enforcement** | **Enforcement**<br>1. Has the entity established procedures for enforcement (sanctions) if an agency or authorized user is suspected of being or has been found to be in noncompliance with the laws and policies, including the entity's P/CRCL policy, when established? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |
| **O. Training** | 1. Will the entity require any individual having physical or logical access to entity information to participate in training programs regarding the implementation of and adherence to the P/CRCL policy? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |
| | 2. Will the entity's privacy training program cover the purpose of the policy, substance and intent of the provisions of the policy, impact of infractions, and possible penalties for violations? | System Administrator OR Privacy and Civil Liberties Officer/Legal Counsel | | | |

# Appendix B—Terms and Definitions

The following is a list of primary terms and definitions used throughout this template. These terms may also be useful in drafting the definitions section of the center's privacy, civil rights, and civil liberties (P/CRCL) policy.

**Access—**Information access is being able to get to (usually having permission to use) particular information on a computer. Web access means having a connection to the Internet through an access provider or an online service provider.

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

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

**Acquisition—**The means by which an ISE participant obtains information through the exercise of its authorities; for example, through human intelligence collection or from a foreign partner. For the purposes of this definition, acquisition does not refer to the obtaining of information widely available to other ISE participants through, for example, news reports or to the obtaining of information shared with them by another ISE participant who originally acquired the information.

**Agency—**See Originating Agency, Owning Agency, Participating Agency, Source Agency, Submitting Agency.

**Analysis (law enforcement)—**The review of information and its comparison to other information to determine the meaning of the data in reference to a criminal investigation or assessment.

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

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

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

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

**Biometrics—**A general term used alternatively to describe a characteristic or a process. (1) As a characteristic: a measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition. (2) As a process: automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics. See Glossary, Facial Identification Scientific Working Group (FISWG), Version 1.1, February 2, 2012, https://www.fiswg.org/FISWG_Glossary_v1.1_2012_02_02.pdf.

**Civil Liberties—**According to the U.S. Department of Justice's Global Justice Information Sharing Initiative, the term "civil liberties" refers to fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of

individuals.[8] They are the freedoms that are guaranteed by the Bill of Rights—the first ten amendments to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference.

**Civil Rights—**The term "civil rights" refers to those rights and privileges of equal protection that government entities must afford to all individuals in the United States regardless of race, ethnicity, gender, national origin, religion, sexual orientation, gender identity, or other characteristics unrelated to the worth of the individual. Protection of civil rights means that government entities will take action to ensure that individuals are not discriminated against on the basis of any federally or state protected characteristic. For example, a state may have constitutional or statutory language regarding parental status. Generally, the term "civil rights" involves positive (or affirmative) government action to protect against infringement, while the term "civil liberties" involves restrictions on government.[9]

**Collect—**For purposes of this document, "gather" and "collect" mean the same thing.

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

**Confidentiality—**Refers to the obligations of individuals and institutions to appropriately use information and data under their control once they have been disclosed to them and in accordance with applicable data security laws and policies.

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

**Criminal Activity—**A behavior, an action, or an omission that is punishable by criminal law.

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

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

**Data Breach—**The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for a purpose other than the authorized purpose.

The center's response to a data breach may be addressed in state law or agency policy. This may include incidents such as:

- Theft or loss of digital media—including computer tapes, hard drives, or laptop computers containing such media—upon which such information is stored unencrypted; posting such information on the Internet.
- Unauthorized employee access to certain information.
- Moving such information to a computer otherwise accessible from the Internet without proper information security precautions.

[8] Civil Rights and Civil Liberties Protections Guidance, at 4 (August 2008), available at https://www.dni.gov/files/ISE/documents/DocumentLibrary/Privacy/CR-CL_Guidance_08112008.pdf.
[9] The definition of "civil rights" is a modified version of the definition contained in the *National Criminal Intelligence Sharing Plan* (NCISP), at pp. 5–6, available at https://it.ojp.gov/documents/National_Criminal_Intelligence_Sharing_Plan.pdf, and Civil Rights and Civil Liberties Protections Guidance, at 5, available at https://www.dni.gov/files/ISE/documents/DocumentLibrary/Privacy/CR-CL_Guidance_08112008.pdf.

- Intentional or unintentional transfer of such information to a system that is not completely open but is not appropriately or formally accredited for security at the approved level, such as unencrypted email.
- Transfer of such information to the information systems of a possibly hostile agency or an environment where it may be exposed to more intensive decryption techniques.

**Data Protection—**Encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, receipt, use, dissemination, retention, purging, and protection of information.

**Data Quality—**Refers to various aspects of the information: the accuracy and validity of the actual values of the data, information structure, and database/information repository design. Traditionally, the basic elements of data quality have been identified as accuracy, completeness, currency, reliability, and context/meaning. Today, data quality is being more fully described in multidimensional models, expanding conventional views of the topic to include considerations of accessibility, security, and privacy. This concept is also addressed as one of the Fair Information Practice Principles (FIPPs), Data Quality/Integrity. See Appendix G for further background on the FIPPs.

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

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

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

**Evaluation**—An assessment of the reliability of the source and accuracy of the raw data.

**Fair Information Practice Principles (FIPPs)—**FIPPs are a set of internationally recognized principles that inform information privacy policies, both within government and the private sector. Although specific articulations of the FIPPs vary and have evolved since their genesis in the 1970s, core elements are consistent among nations, states, and economic sectors. These core elements are incorporated into information privacy laws, policies, and governance documents around the world. They provide a straightforward description of underlying privacy and information exchange principles and a simple framework for the legal use that needs to be done with regard to privacy in integrated justice systems. Because of operational necessity, it may not always be possible to apply all of the principles equally. For example, the Individual Participation Principle (#8) may be of limited applicability in justice entities, since they do not generally engage with individuals. That said, integrated justice systems should endeavor to apply the FIPPs where practicable.

The eight principles are:

1. Purpose Specification
2. Data Quality/Integrity (see definition)
3. Collection Limitation/Data Minimization
4. Use Limitation
5. Security Safeguards (see definition)
6. Accountability/Audit
7. Openness/Transparency
8. Individual Participation

See Appendix G for further background on the FIPPs.

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

**Fusion Center**—Defined in the ISE-SAR Functional Standard, Version 1.5.5 as "[a] collaborative effort of two or more Federal, State, local, tribal, or territorial (SLTT) government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity." (Source: Section 511 of the 9/11 Commission Act). State and major urban area fusion centers serve as focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information between the federal government and SLTT and private sector partners.

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

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

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

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

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

**Information Sharing Environment (ISE**)—In accordance with Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended, the ISE is a conceptual framework composed of the policies, procedures, and technologies linking the resources (people, systems, databases, and information) of SLTT agencies; federal agencies; and the private sector to facilitate terrorism-related information sharing, access, and collaboration.

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

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

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

**Joint Terrorism Task Forces (JTTFs)—**The Federal Bureau of Investigation's (FBI) JTTFs are interagency task forces designed to enhance communication, coordination, and cooperation in countering terrorist threats. They combine the resources, talents, skills, and knowledge of federal, state, territorial, tribal, and local law enforcement and homeland security agencies, as well as the Intelligence Community, into a single team that investigates and/or responds to terrorist threats. The JTTFs execute the FBI's lead federal agency responsibility for investigating terrorist acts or terrorist threats against the United States.

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

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

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

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

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

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

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

**Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)—**The NSI establishes standardized processes and policies that provide the capability for federal, SLTT, campus, and railroad law enforcement and homeland security agencies to share timely, relevant ISE-SARs through a distributed information sharing system that protects privacy, civil rights, and civil liberties.

**Nationwide SAR Initiative (NSI) SAR Data Repository (SDR)—**The NSI SDR consists of a single data repository, built to respect and support originator control and local stewardship of data, which incorporates federal, state, and local retention policies. Within the SDR, hosted data enclaves extend this approach to information management and safeguarding practices by ensuring a separation of data across participating agencies.

**Need to Know—**As a result of jurisdictional, organizational, or operational necessities, access to sensitive information or intelligence is necessary for the conduct of an individual's official duties as part of an organization

that has a right to know the information to perform or assist in a law enforcement, homeland security, or counterterrorism activity or other lawful and authorized government activity, such as to further an investigation or meet another law enforcement requirement.

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

**Nonvalidated Information—**A tip or lead (including a SAR) received by the center that has been determined to be false or inaccurate or otherwise determined not to warrant additional action and/or maintenance.

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

**Owning Agency/Organization—**The organization that owns the target associated with the suspicious activity.

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

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

**Personally Identifiable Information—**"Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."[10]

**Preoperational Planning—**As defined in ISE-SAR Functional Standard, Version 1.5.5, "preoperational planning describes activities associated with a known or particular planned criminal operation or with terrorist operations generally."

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

**Privacy, Civil Rights, and Civil Liberties (P/CRCL) Policy—**A printed, published statement that articulates the policy position of an organization on how it handles the PII that it maintains and uses in the normal course of business. The policy should include information relating to the processes of information collection, receipt, access, use, dissemination, retention, and purging. It is likely to be informed by the Fair Information Practice Principles (FIPPs). The purpose of the P/CRCL policy is to articulate that the center will adhere to those legal requirements and center policy determinations that enable collection, receipt, access, use, dissemination, retention, and purging of information to occur in a manner that protects personal privacy interests. A well-developed and implemented P/CRCL policy uses justice entity resources wisely and effectively; protects the center, the individual, and the public; and promotes public trust.

**Privacy Impact Assessment (PIA)—**A process by which an entity can examine the P/CRCL risks in the justice entity's information system and sharing activities. In general, a PIA evaluates the process through which PII is

[10] For further information about the breadth of PII and how to perform an assessment of the specific risk that an individual can be identified using the information, see Revision of Office of Management and Budget Circular A-130: Managing Information as a Strategic Resource, July 2016, https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.

collected, stored, protected, shared, managed, and purged. By completing a PIA, entities are able to identify P/CRCL vulnerabilities and to address and mitigate them through the design and implementation of policies.

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

**Protected Information—**For the nonintelligence community, protected information is information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and laws of the United States.

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

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

**Public—**Public includes:

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

Public does not include:

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

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

**Purge—**A term that is commonly used to describe methods that render data unrecoverable in a storage space or to destroy data in a manner that it cannot be reconstituted. There are many different strategies and techniques for data purging, which is often contrasted with data deletion (e.g., made inaccessible except to system administrators or other privileged users.)

**Reasonably Indicative—**This operational concept for documenting and sharing suspicious activity takes into account the circumstances in which that observation is made which creates in the mind of the reasonable

observer, including a law enforcement officer, an articulable concern that the behavior may indicate preoperational planning associated with terrorism or other criminal activity. It also takes into account the training and experience of a reasonable law enforcement officer, in cases in which an officer is the observer or documenter of the observed behavior reported to a law enforcement agency.

**Record—**Any item, collection, or grouping of information that includes PII and is collected, received, accessed, used, disseminated, retained, and purged by or for the collecting agency or organization.

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

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

**Retention—**Refer to Storage.

**Right to Information Privacy—**The right to be left alone, in the absence of some reasonable public interest in collecting, accessing, retaining, and disseminating information about an individual's activities. Invasion of the right to privacy can be the basis for a lawsuit for damages against the individual or entity violating an individual's privacy.

**Right to Know—**A requirement for access to specific information to perform or assist in a lawful and authorized governmental function. Right to know is determined by the mission and functions of a law enforcement, homeland security, counterterrorism, or other lawful and authorized government activity or the roles and responsibilities of particular personnel in the course of their official duties.

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

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

**Source Agency/Organization—**Defined in the ISE-SAR Functional Standard, Version 1.5.5, source agency refers to the agency or entity that originates the SAR (examples include a local police department, a private security firm handling security for a power plant, and a security force at a military installation). The source organization will not change throughout the life of the SAR.

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

- Storage is frequently used to mean the devices and data connected to the computer through input/output operations—that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-computer storage. This is probably the most common meaning in the IT industry. In a more formal usage, storage has been divided into (1) primary storage, which holds data in memory (sometimes called random access memory, or RAM) and other "built-in" devices, such as the processor's L1 cache, and (2) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations. Primary storage is much faster to access than secondary storage because of the proximity of the storage to the processor or because of the nature of the storage devices. On the other hand, secondary storage can hold much more data than primary storage.

With regard to the ISE, storage (or retention) refers to the storage and safeguarding of terrorism-related information—including homeland security information, terrorism information, and law enforcement information relating to terrorism or the security of our homeland—by both the originator of the information and any recipient of the information.

**Submitting Agency/Organization—**The organization that actuates the push of the ISE-SAR to the NSI community. The submitting organization and the source organization may be the same.

**Suspicious Activity—**Defined in the ISE-SAR Functional Standard, Version 1.5.5 as "[o]bserved behavior reasonably indicative of preoperational planning associated with terrorism or other criminal activity." Examples of suspicious activity include surveillance, photography of sensitive infrastructure facilities, site breach or physical intrusion, cyberattacks, testing of security, etc.

**Suspicious Activity Report (SAR)—**Defined in the ISE-SAR Functional Standard, Version 1.5.5 as "[o]fficial documentation of observed behavior reasonably indicative of preoperational planning associated with terrorism or other criminal activity." Suspicious activity report (SAR) information offers a standardized means for feeding information repositories or data analysis tools. Patterns identified during SAR information analysis may be investigated in coordination with the reporting agency and, if applicable, a state or regional fusion center. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor is it designed to support interagency calls for service.

**Terrorism Information—**Consistent with Section 1016(a)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), all information relating to (a) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or materials support, or activities of foreign **or** international terrorist groups or individuals **or** of domestic groups **or** individuals involved in transnational terrorism; (b) threats posed by such groups or individuals to the United States, United States persons, or United States interests or to those interests of other nations; (c) communications of or by such groups or individuals; or (d) other groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

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

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

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

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

to law enforcement and being extremely valuable depending on the availability of time and resources to determine its meaning.

**Unvalidated information—**A tip or lead (including a SAR) received by the center that has not yet been reviewed to determine further action or maintenance.

**U.S. Person—**Executive Order 12333 states that a "United States person" means a U.S. citizen, an alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially composed of U.S. citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.

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

**Validated Information—**A tip or lead (including a SAR) that has been reviewed and, when appropriate, combined with other information or further vetted and is determined to warrant additional action, such as investigation or dissemination, and/or maintenance according to the applicable record retention policy.

# Appendix C—Model Legislation

**Section 1.100 Purpose**

To ensure that all criminal justice data information systems developed, procured, or significantly modified minimize the risk of inappropriate impacts on the privacy of individuals, the "Data System Privacy Review Act" is enacted.

**Section 1.200 Definitions**

a. "Criminal justice agency" has the meaning given provided in Section **[insert citation to appropriate state law]** and includes courts.

b. "Information system" includes any technology system or project that collects, maintains, or disseminates personally identifiable data.

c. "Personally identifiable data" means data from which an individual human being can be uniquely identified including but not limited to:

   1. First and last name

   2. Physical address

   3. Email address

   4. Telephone number

   5. Social security number

   6. Credit card information

   7. Bank account information

   8. Any combination of personally identifiable information that could be used to determine an individual's identity

d. "Privacy Impact Assessment" or "assessment" means answers to a series of questions approved by **[insert authority]** to evaluate how personally identifiable information is collected, stored, protected, shared, and managed by an electronic information system or online collections application.

**Section 1.300 General Provisions**

a. A criminal justice agency or court developing, procuring, or significantly modifying an existing information data system containing personally identifiable information shall complete a Privacy Impact Assessment authorized by **[insert authority]** before the system is implemented.

b. Completed assessments shall be posted on the criminal justice agency's website and maintained in the agency's principal office for four years.

c. Completed assessments shall be submitted to **[insert authority; e.g., chief information officer, chief privacy officer, attorney general's office]** for review and approval.

d. The **[insert authority]** shall report annually on January 15 to the Legislature all of the assessment completed in the prior year.

**Section 1.400 Penalties**

a. Agencies or courts failing to complete and submit a completed assessment in a timely manner may forfeit current and future funding for information technology systems.

Criminal justice agencies and system proponents could also encourage adoption of the following executive order (see Appendix D) by their state's governor.

# Appendix D—Sample Executive Order

**Note:** The authors of this PIA Guide acknowledge that the following sample executive order may require modification for use by local (county, city) or tribal governments, since each has its own unique political structure and system of government. Also, the language may be customized as a resolution to reflect an entity's commitment to support privacy protections, such as through the completion of a PIA and development and implementation of an entity privacy policy, as opposed to an official order.

## Improving Data Protection and Security by State Agencies

I, GOVERNOR _____ OF THE STATE OF _____, by virtue of the authority vested in me by the Constitution and applicable laws, do hereby issue this executive order:

WHEREAS, _____'s state agencies are the data stewards of personally identifiable information about its citizens in their possession and have a duty to protect that data from misuse, and appropriate management of sensitive information, including social security numbers, driver's license numbers, financial account numbers, and other similar sensitive personal information, respects the privacy of those individuals associated with that data;

WHEREAS, *sensitive information that is not adequately protected can cause individuals to suffer a variety of consequences, including invasion of privacy, personal embarrassment, stalking, harassment, identity theft, or other criminal misuses of their data*;

WHEREAS, identity theft costs our nation's citizens and businesses billions of dollars in losses each year, and misuse of sensitive data can also place individuals at risk for harassment, stalking, and other criminal acts;

NOW THEREFORE, I hereby order that:

1. The state's Chief Information Officer will be responsible for coordinating the implementation of improved privacy measures.

2. Within 90 days, the state's Chief Information Office shall develop and disseminate a Privacy Impact Assessment (PIA) Directive for use by state agencies for all new or significantly modified information data systems. The Directive will address what information is to be collected, why the information is being collected, intended use of the information, with whom the information will be shared, what opportunities individuals have to decline to provide information or to consent to particular uses of the information (other than required or authorized uses), how individuals can grant consent, and how the information will be secured.

3. Within one year, all state agency heads shall conduct Privacy Impact Assessments on all existing systems that maintain personally identifiable information to include names and addresses, social security numbers, driver's license numbers, and financial institution account information of more than (10,000) individuals.

4. Prior to requesting any state funds to develop, procure, or significantly modify a data system, state agency heads shall conduct a Privacy Impact Assessment.

5. Completed Privacy Impact Assessments shall be prominently posted on a state agency's website for at least two years.

Pursuant to **[insert cite]**, this executive order will be effective until **[insert date]**.

**This page intentionally left blank.**

# Appendix E—Office of Management and Budget Memorandum

**(OMB M-03-022), OMB Guidance for Implementing the Privacy Provision of the E-Government Act of 2002**

In general, PIAs are required to be performed and updated as necessary when a system change creates new privacy risks. For example:

**a. Conversions**—when converting paper-based records to electronic systems;

**b. Anonymous to Non-Anonymous**—when functions applied to an existing information collection change anonymous information into information in identifiable form;

**c. Significant System Management Changes**—when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system:

- For example, when an agency employs new relational database technologies or Web-based processing to access multiple data stores; such additions could create a more open environment and avenues for exposure of data that previously did not exist.

**d. Significant Merging**—when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases, or otherwise significantly manipulated:

- For example, when databases are merged to create one central source of information; such a link may aggregate data in ways that create privacy concerns not previously at issue.

**e. New Public Access**—when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public;

**f. Commercial Sources**—when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources. (Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement);

**g. New Interagency Uses**—when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives; in such cases, the lead agency should prepare the PIA;

- For example, the Department of Health and Human Services, the lead agency for the Administration's Public Health Line of Business (LOB) Initiative, is spearheading work with several agencies to define requirements for integration of processes and accompanying information exchanges. HHS would thus prepare the PIA to ensure that all privacy issues are effectively managed throughout the development of this cross-agency IT investment.

**h. Internal Flow or Collection**—when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form:

- For example, agencies that participate in E-Gov initiatives could see major changes in how they conduct business internally or collect information, as a result of new business processes or E-Gov requirements. In most cases the focus will be on integration of common processes and supporting data. Any business change that results in substantial new requirements for information in identifiable form could warrant examination of privacy issues.

**i. Alteration in Character of Data**—when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information).

**This page intentionally left blank.**

# Appendix F—Information and Resources About Social Media

In response to the increased use of social media websites (such as Facebook, Twitter, LinkedIn, YouTube, and blogs), federal, state, local, tribal, and territorial agencies and law enforcement organizations have embraced social media tools for various purposes, including:

- **Communications**—increasing public awareness and outreach to and engagement with constituents and fostering greater transparency and connections within communities.
- **Networking**—connecting with other law enforcement organizations and associations.
- **Investigations**—gathering open source information or evidence to support a legitimate law enforcement purpose.
- **Notifications**—providing time-sensitive notifications to the public.

From a privacy perspective, the general public may not differentiate between an organization's various uses of social media. It is in the interest of federal, state, local, tribal, and territorial organizations to proactively notify the public and their specific constituent bodies of the organization's intended uses of social media tools.

## Guidance on Privacy Impact Assessments for Social Networking

In June 2010, the Office of Management and Budget (OMB) issued Memorandum 10-23, *Guidance for Agency Use of Third-Party Websites and Applications* (June 25, 2010), which updates the guidance of OMB Memorandum 03-22 (*OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (September 30, 2003)) regarding Privacy Impact Assessments (PIA). OMB Memorandum 10-23 directs federal agencies planning the use of third-party social media sites and applications to prepare an adapted PIA whenever an agency's use of a third-party website or application makes personally identifiable information (PII) available to the agency. In December 2011, OMB, in collaboration with the Privacy Committee of the federal Chief Information Officers (CIO) Council, issued additional guidance and a model template PIA for use by federal agencies engaging in the use of social media.

Both OMB Memorandum 10-23 and the December 2011 OMB Model PIA guidance recommend addressing the following questions when developing a PIA for social media:

i. The specific purpose of the agency's use of the social networking website or application.

ii. Any PII that is likely to become available to the agency through public use of the social networking website or application.

iii. The agency's intended or expected use of PII.

iv. With whom the agency will share PII.

v. Whether and how the agency will maintain/retain PII and for how long.

vi. How the agency will secure PII that it uses or maintains.

vii. How safeguards will be used to prevent unauthorized uses of PII.

viii. What other privacy risks exist and how the agency will mitigate those risks.

The adapted PIA should also address whether the agency's activities will affect legal and regulatory requirements. An organization should ensure that stakeholders with a role in the organization's use of social

media are engaged in the development of a PIA for social media, to include privacy, security, records management, and public affairs officers.

## Other Considerations

Organizations must also consider the boundaries between employees' use of social media for authorized official purposes and personal use. While law enforcement officers and public employees have constitutional rights to freedom of speech, courts have grappled with distinctions between statements made in an official capacity versus those made as a private citizen. Organizations are encouraged to examine and update their internal policies and procedures to address the personal use of social media sites by officers and/or employees. Organizations should also train officers and employees on the use of social media websites and applications to avoid the potential for an employee's personal use of social media to be detrimental to the organization.

## Resources

- International Associational of Chiefs of Police (IACP) Center for Social Media, www.iacpsocialmedia.org
- Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations (February 2013), https://it.ojp.gov/gist/132/File/Developing%20a%20Policy%20on%20the%20Use%20of%20Social%20Media%20in%20Intelligence%20and%20Investigative%20Activities_compliant.pdf
- Real-Time Open Source Analysis (ROSA) Resource Guide (July 2017), https://it.ojp.gov/GIST/1200/Real-Time-and-Open-Source-Analysis--ROSA--Resource-Guide
- IACP Model Policy for Social Media, http://www.iacpsocialmedia.org/getting-started/policy-development/
- OMB Memorandum 10-23, *Guidance for Agency Use of Third-Party Websites and Applications* (June 25, 2010), https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf
- OMB Memorandum for the Chief Information Officers, Model Privacy Impact Assessment for Agency Use of Third Party websites and Applications (December 29, 2011), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/inforeg/inforeg/info_policy/model-pia-agency-use-third-party-websites-and-applications.pdf

## Example of Social Media Privacy Impact Assessments

- DOJ Adapted Privacy Impact Assessment for Use of Third-Party Social Media Tools to Communicate with the Public, https://www.justice.gov/Use_Third_Part_Social_Media_Tools/download
- DHS Social Networking PIA, https://www.dhs.gov/publication/dhsallpia-031-use-social-networking-interactions-and-applications-0

# Appendix G—Fair Information Practice Principles

Fair Information Practice Principles (FIPPs) are a set of internationally recognized principles that inform information privacy policies within both government and the private sector.

Although specific articulations of the FIPPs vary and have evolved since their genesis in the 1970s, core elements are consistent among nations, states, and economic sectors. These core elements are incorporated into data privacy laws, policies, and governance documents around the world. For example, the core elements of the FIPPs can be found:

- At the heart of the Privacy Act of 1974, which applies these principles to U.S. federal agencies.[11]
- Mirrored in many states' laws and in justice entities' privacy policies.
- In the ISO/IEC 29100 Privacy Framework, which has been adopted by numerous foreign countries and international organizations.

The following formulation of the FIPPs is used and implemented for the Information Sharing Environment (ISE) by the U.S. Department of Homeland Security (DHS).[12] Note, however, that under certain circumstances, the FIPPs may be superseded by authorities paralleling those provided in the federal Privacy Act; state, local, tribal, or territorial law; or center policy.

1. **Purpose Specification—**Agencies should specifically articulate the authority that permits the collection of PII. The purpose(s) for which PII is collected should be specified at the time of data collection. Subsequent use of this data should be limited to the original purpose for which the PII was collected (or other purposes compatible with the original collection purpose).

   Implementing the Purpose Specification Principle—Agencies are bound by specific constitutional and statutory authorities that circumscribe their ability to collect PII. The following are examples of ways agencies may implement this principle:

   - Ensure that a valid lawful purpose exists and is documented for all collection of PII.
   - Include the source and authority for the data so that access restrictions can be applied.
   - Upon receipt of data containing PII from third parties, if possible, identify the purpose for which it was collected initially and limit agency use to only those uses compatible with the original purpose supporting collection.
   - Ensure that metadata or other tags are associated with the data as it is shared.
   - Institute a two-individual review and approval process to consider any Privacy Act or other legal or policy limitation before permitting use or sharing of data for purposes other than that for which it was collected.

2. **Data Quality/Integrity—**PII collected should be relevant to the purposes identified for its use and should be accurate, complete, and up to date.

   Implementing the Data Quality/Integrity Principle—One important way to minimize potential downstream P/CRCL concerns is to ensure that any information collected, stored, and disseminated is accurate. This includes ensuring that the information provides sufficient context for any PII. Possible approaches include:

   - Properly labeling PII.
   - Determining a policy for safeguarding PII if there are "mixed" databases (i.e., those databases with PII on U.S. individuals and others, regardless of nationality).
   - Instituting a source verification procedure to ensure that reporting is based only on authorized data.

[11] 5 U.S.C. § 552a.
[12] 6 U.S.C. § 142.

- Reconciling and updating PII whenever new relevant information is collected.
- Developing a protocol for ensuring that data corrections are passed to those entities with which information has been shared.
- Creating a documented process for identifying and addressing situations in which data has been erroneously received, is inaccurate, or has been expunged.

3. **Collection Limitation/Data Minimization—**PII should be collected only if the data is directly relevant and necessary to accomplish the specified purpose. PII should be obtained by lawful and fair means and retained only as long as is necessary to fulfill the specified purpose.

   Implementing the Collection Limitation/Data Minimization Principle—Collection limitation may be implemented by:

   - Designing a data storage system to pull data for review and then, if appropriate, automatically purging data after the specified retention period has been reached.
   - Limiting data field elements to only those that are relevant.
   - Ensuring that all distributed reports and products contain only PII that is relevant and necessary (nothing extraneous or superfluous).
   - Ensuring that all shared information with PII meets required thresholds for sharing, such as reasonable suspicion.

4. **Use Limitation—**PII should not be disclosed, made available, or otherwise used for purposes other than those specified except (a) with the consent of the individual or (b) by the authority of law.

   Implementing the Use Limitation Principle—Sharing information should be tempered by adherence to key principles such as "authorized access." Use limitation may be implemented by:

   - Limiting users of data to those with credential-based access.
   - Requiring that justifications be entered and logs maintained for all queries with sensitive PII and that an internal review process of those logs take place at specified intervals.
   - Requiring senior analysts to review all reports that use PII before dissemination to ensure (a) that PII is relevant and necessary and (b) that the recipient is authorized to receive the information in the performance of an authorized activity.
   - Prior to sharing information, verify that partners have a lawful purpose for requesting information.
   - Creating multiple use-based distribution lists and restricting distribution to those authorized to receive the information.

5. **Security/Safeguards—**Agencies should institute reasonable security safeguards to protect PII against loss, unauthorized access, destruction, misuse, modification, or disclosure.

   Implementing the Security/Safeguards Principle—This principle can be implemented by:

   - Maintaining up-to-date technology for network security.
   - Ensuring that access to data systems requires that users meet certain training and/or vetting standards and that such access be documented and auditable.
   - Ensuring that physical security measures are in place, such as requiring an identification card, credentials, and/or passcode for data access; disabling computers' USB ports; and implementing firewalls to prevent access to commercial email or messaging services.
   - Implementing a protocol with technical and manual safeguards to ensure the accuracy and completeness of data system purges when records are deleted at the end of their retention period.
   - Ensuring that data system purge protocols include complete record deletion on all backup systems.
   - Transitioning older repositories into more modern systems to improve access controls.
   - Masking data so that it is viewable only to authorized users.

- Maintaining an audit log to record when information is accessed and by whom for review by senior staff at specified intervals.
- Requiring authorized users to sign nondisclosure agreements.

6. **Accountability/Audit—**Agency personnel and contractors are accountable for complying with measures implementing the FIPPs, for providing training to all employees and contractors who use PII, and for auditing the actual use and storage of PII.

   Implementing the Accountability/Audit Principle—Strong policies must not only be in place but also be effectively implemented. Accountability can be demonstrated by:

   - Ensuring that upon entry for duty, all staff take an oath to adhere to the privacy and civil liberties protections articulated in the center's or host agency's mission, core values statements, other key documents, and/or the U.S. Constitution.
   - Conducting effective orientation and periodic refresher training, including P/CRCL protections, for all individuals handling PII.
   - Tailoring training to specific job functions, database access, or data source/storage requirements.
   - Conducting regular audits of all systems in which records are kept to ensure compliance with the P/CRCL policies and all legal requirements.
   - Following a privacy incident handling procedure for any data breaches or policy violations.
   - Denying database access to individuals until they have completed mandatory systems access training (including training for handling of PII), show a mission need for access, and have any necessary clearances.
   - Developing targeted and consistent corrective actions whenever noncompliance is found.

7. **Openness/Transparency—**To the extent feasible, agencies should be open about developments, practices, and policies with respect to the collection, use, dissemination, and maintenance of PII. Agencies should publish information about policies in this area, including the P/CRCL policy, and contact information for data corrections and complaints.

   Implementing the Openness/Transparency Principle—Agencies can implement the Openness/Transparency principle by:

   - Providing reports to an internal or external oversight body concerned with P/CRCL issues, including P/CRCL audit results.
   - Publishing the P/CRCL policy and redress procedures.
   - Meeting with community groups through initiatives or through other opportunities to explain the agencies' mission and P/CRCL protections.
   - Responding in the fullest way possible to freedom of information and/or sunshine requests and fully explaining any denial of information requests from the public.
   - Conducting and publishing Privacy Impact Assessments (PIAs) in advance of implementing any new technologies that affect PII, thereby demonstrating that P/CRCL issues have been considered and addressed.

8. **Individual Participation—**To the extent practicable, involve the individual in the process of using PII and seek individual consent for the collection, use, dissemination, and maintenance of PII. Agencies should also provide mechanisms for appropriate access, correction, and redress regarding their use of PII.

   Implementing the Individual Participation Principle—To the extent appropriate, agencies can implement the Individual Participation principle by:

- Collecting information directly from the individual, to the extent possible and practical.
- Providing the individual with the ability to find out whether an agency maintains a record relating to him or her and, if not (i.e., access and/or correction is denied), then providing the individual with notice as to why the denial was made and how to challenge such a denial.
- Putting in place a mechanism by which an individual is able to prevent information about him or her that was obtained for one purpose from being used for other purposes without his or her knowledge.