INFORMATION SHARING ENVIRONMENT

Framework of Considerations for Streamlining the Terrorism-Related Information Sharing and Access Agreement Development Process and Incorporating Privacy, Civil Rights, and Civil Liberties Best Practices

NATIONAL SECURITY THROUGH RESPONSIBLE INFORMATION SHARING

May 2015

FRAMEWORK OF CONSIDERATIONS FOR STREAMLINING THE TERRORISM-RELATED INFORMATION SHARING AND ACCESS AGREEMENT DEVELOPMENT PROCESS AND INCORPORATING PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES BEST PRACTICES

I. Introduction

In response to the U.S. government's *Data Aggregation Capabilities Applicable to Terrorism* report, the Privacy and Civil Liberties (P/CL) Subcommittee of the Information Sharing and Access Interagency Policy Committee has developed this *Framework of Considerations for Streamlining the Terrorism-Related Information Sharing and Access Agreement Development Process and Incorporating Privacy, Civil Rights, and Civil Liberties Best Practices* (Framework) in an effort to define a common methodology for developing information sharing and access agreements (ISAAs). In order to streamline the development process and to promote best practices, the Framework will recommend preliminary steps and identify key privacy, civil rights, and civil liberties (P/CRCL) issues to be considered early in the development of ISAAs to avoid delayed or derailed agreements.

This Framework is not meant to cover every possible P/CRCL issue that may arise in the Information Sharing Environment (ISE).[1] Rather, it highlights common issues related to the acquisition, use, maintenance, and dissemination of personally identifiable information (PII), including "Protected Information," by ISE mission partners.

This Framework is intended to be used as a resource by federal agencies and their employees who are participating or expecting to participate in the ISE and who have ISAA responsibilities, including parties responsible for oversight of an ISAA. ISAA stakeholders are urged to begin identifying and working through the potential P/CRCL issues in the early stages of ISAA development. By doing so, stakeholders will not only improve information sharing by minimizing delays in the development and implementation of ISAAs but also ensure that appropriate and robust P/CRCL safeguards are built into the ISAAs with federal ISE mission partners.

To supplement this Framework, the P/CL Subcommittee has developed a worksheet reflecting core P/CRCL protections. This worksheet is appended to this Framework as Appendix D.

[1] The ISE is an approach that facilitates the sharing of terrorism-related information. See Section 1016(a) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended, and codified at 6 U.S.C. § 485(a). In the ISE, "terrorism-related information" includes terrorism information, homeland security information (including weapons of mass destruction information), and law enforcement information related to terrorism.

II. Background on Protecting P/CRCL in the ISE

A. Authorities

Section 1016(d)(2)(A) of the Intelligence Reform and Terrorism Prevention Act (IRTPA)[2] required the President to issue guidelines that "protect privacy and civil liberties in the development and use of the ISE." The President included this IRTPA mandate in Section 1 of Executive Order 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans (October 25, 2005), wherein the President provided that "to the maximum extent consistent with applicable law, [federal] agencies shall . . . give the highest priority to . . . the interchange of terrorism information among agencies . . . [and shall] protect the freedom, information privacy, and other legal rights of Americans in the conduct of [such] activities . . . ." In order to implement the requirements of the IRTPA and other executive orders, the President, in Guideline 5 of his Presidential Memorandum of December 16, 2005, directed the U.S. Attorney General (AG) and the Director of National Intelligence to develop "guidelines designed to be implemented by executive departments and agencies to ensure that the information privacy and other legal rights of Americans are protected in the development and use of the ISE, including the acquisition, access, use, and storage of personally identifiable information." The resulting *Guidelines to Ensure That the Information Privacy and Other Legal Rights of Americans Are Protected in the Development and Use of the Information Sharing Environment* (ISE Privacy Guidelines) were approved by the President and issued by the Program Manager for the ISE (PM-ISE) on December 4, 2006.[3]

The ISE Privacy Guidelines create a government-wide protection framework for P/CRCL throughout the ISE and require core P/CRCL protections to be implemented by ISE agencies in a manner consistent with their own legal authorities and mission requirements. Section 2(a) of the ISE Privacy Guidelines specifically requires that "all agencies shall, without exception, comply with the Constitution and all applicable laws and Executive orders relating to Protected Information in the ISE." In Section 1(b) of the Guidelines, *Protected Information* is defined as "information about American citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and federal laws of the United States." These "other legal protections" derive primarily from the civil liberties guaranteed by the Constitution of the United States and the civil rights laws of the United States. Section 1(b) also states that Protected Information includes (for the Intelligence Community [IC]) "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

---

[2] See IRTPA, Pub. L. 108-458, December 17, 2004, as amended by the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. 110–53, August 3, 2007.

[3] The ISE Privacy Guidelines may be found at http://ise.gov/sites/default/files/PrivacyGuidelines20061204.pdf. The Compliance Review Self-Assessment Checklist was developed by the Privacy and Civil Liberties Subcommittee to assist Federal ISE agencies in conducting a self-assessment of the agency's implementation of its ISE privacy protection policy and the *ISE Privacy Guidelines* requirements. The Checklist, along with other resources relating to the P/CRCL protection framework for the ISE, may be located at http://ise.gov/privacy-civil-rights-and-civil-liberties-protection-framework.

by Executive order, international agreement, or other similar instrument, should be covered by [the] guidelines."

B. What Is Information Privacy**?**

With respect to the ISE, a primary focus is on "information privacy," a subset of the privacy protections derived from various sources of U.S. law. Information privacy generally relates to the ability to control information about oneself. The Privacy Act of 1974 protects the information privacy of U.S. citizens and lawful permanent residents (LPRs),[4] imposing obligations on federal agencies that acquire and administer information about individuals and affording individuals certain rights with respect to information these agencies collect about individuals. The Privacy Act embraces a set of Fair Information Practice Principles (FIPPs) embedded in its provisions. The FIPPs, which are also called Fair Information Practices, provide the framework used by P/CL officials for identifying and mitigating privacy risks related to the acquisition, maintenance, use, or dissemination of information about individuals through the application of core principles, such as notice, right of access and correction, collection limitations, data quality, consent to sharing, security, and accountability.[5] Agency policies may enumerate the FIPPs slightly differently, but the core principles form the foundation of a widely accepted framework that is mirrored in the laws of many U.S. states, foreign nations, and international organizations. Privacy interests requiring protection may include preventing the misuse of personal information, which could result in harm or unfairness to an individual. These protections foster public trust by safeguarding what is generally called "PII" and enhance mission effectiveness and counterterrorism efforts by improving the quality of the information on which analytic and investigative judgments are made.

C. What Are Civil Rights and Civil Liberties?

The term *civil liberties* is broader than the concept of privacy and, in fact, embraces privacy. Basic civil liberties cover a broad range of rights established by the first ten amendments to the U.S. Constitution, known as the Bill of Rights, including (but not limited to): (1) Freedom of Association, (2) Freedom of Assembly, (3) Freedom of Religion, (4) Freedom of Speech, (5) Due Process of Law, and (6) Right to a Fair Trial.[6]

The term *civil rights,* for the purposes of this Framework, involves proactive action by government to protect against infringement of rights guaranteed by the U.S. Constitution and acts of Congress. The ISE Privacy Guidelines Civil Rights and Civil Liberties Protection Guidance

[4] See 5 U.S.C. § 552a(a)(2) (for purposes of the Privacy Act, the term *individual* refers to "a citizen of the United States or an alien lawfully admitted for permanent residence").
[5] See Appendix A for further information on the FIPPs.
[6] See Attachment B for an overview of the basic civil liberties.

defines these terms further.[7] Depending on an agency's mission, the nature of the data, and the ramifications to protected individuals of sharing information in the ISE, a variety of civil rights laws may be implicated.[8]

D. Privacy/Civil Right and Civil Liberties: How to Frame These Issues in Information Sharing Access Agreements at the Outset

ISAAs will govern the process by which information in shared between agencies; therefore, it is important to begin considering privacy and civil liberties concerns in the initial stages of drafting. The relevant stakeholders should always consider the purpose for sharing the requested information. Another factor that should be considered at the outset is what information the receiving agency needs. The scope and types of information provided should not be broader than necessary to serve the requesting agency's purpose. As discussed in Section V.A.2 below, stakeholders should always ask whether less information could achieve the same result.

Additionally, it is important to incorporate appropriate safeguards regarding dissemination, retention, and data security. Stakeholders must understand any preexisting limitations on dissemination of data as well the intended method for sharing or aggregating the information in order to properly draft an ISAA. Further, the retention section of the ISAA should specifically address how long a receiving agency may retain the data relevant to its mission, and how it must dispose of the information that is not relevant to the mission. The worksheet in Appendix D should be utilized to help ensure the incorporation of privacy and civil liberties protections in the drafting process.

III. What You Need to Know About Developing a Data Sharing/Aggregation Agreement or Initiative Before You Write an ISAA

IRTPA fundamentally altered the federal government's information sharing approach by imposing a dual mandate to share terrorism information ("need to share") while protecting P/CRCL. The IRTPA's "need to share" requirement means that information must be shared "at and across all levels of security."[9] This does not mean, however, that an agency may never limit uses, users, and methods or require safeguards for information that is shared. The need to share is subject to statutory, regulatory, and policy-based limits and requires the development of appropriate safeguards to protect "individuals' privacy and civil liberties" as well as "strong

[7] See Civil Rights and Civil Liberties Protection Guidance, at 5, citing a modified version of the definition contained in the *National Criminal Intelligence Sharing Plan* (NCISP), at 5–6, and available at http://www.ise.gov/sites/default/files/CR-CL_Guidance_08112008.pdf.

[8] This may potentially include (1) the Civil Rights Act of 1964, as amended, 42 U.S.C. § 2000e *et seq*.; (2) the Rehabilitation Act of 1973, Pub. L. 93-112, 29 U.S.C. § 701 *et seq*.; (3) the Equal Educational Opportunities Act of 1974, 20 U.S.C. § 1701 *et seq*.; (4) the Americans with Disabilities Act, 42 U.S.C. § 12101 *et seq*.; (5) the Fair Housing Act, 42 U.S.C. § 3601; (6) the Voting Rights Act of 1965, 42 U.S.C. §§ 1973–1973aa-6 (protecting Americans against racial discrimination in voting); and the Civil Rights of Institutionalized Persons Act, 42 U.S.C. § 1997 *et seq*.

[9] 6 U.S.C. § 485(b)(2)(F).

mechanisms to enhance accountability and facilitate oversight" (e.g., audits, authentication, and access controls).[10]

A. Involve Stakeholders as Soon as Possible

A critical first step to streamlining the ISAA process is the identification of stakeholders who have responsibilities related to the development or implementation of the ISAA. For this process to work effectively and efficiently, an interdisciplinary approach is required. If your agency has an established ISAA management process or a chief information sharing officer, the responsible office may be able to direct you to the appropriate points of contact.

Identifying and engaging the appropriate participants before commencing the development process will not only enhance the ultimate agreement but also help avoid unnecessary delay and ensure privacy protections are built into the agreement from the outset. Essential stakeholders from both the providing and requesting parties[11] include the providing agency, a representative from the office of general counsel, representatives from the office(s) with agency-wide responsibility for P/CRCL or the component-specific P/CRCL officer (as applicable), the information sharing executive at a department level (if any), a representative of the chief information officer, the intended users and business owners,[12] and key points of contacts (e.g., management, technical, and operation and maintenance support process, such as service-level agreements). [13]

Involving P/CRCL professionals early in the development process is likely to assist in preventing unnecessary delays. P/CRCL professionals can facilitate the ISAA process by assessing the concept for the plan, spotting issues early in the development process, and suggesting ways to mitigate potential P/CRCL impacts. For this reason, ISAA stakeholders are urged to fully engage P/CRCL professionals early in the planning stage and to sustain an ongoing consultative relationship thereafter.

Once the stakeholders for the ISAA development process have been identified, consider the review and finalization process. In particular, stakeholders should be tasked to identify officials who will be responsible for reviewing the terms of the contemplated ISAA prior to signature. For planning purposes, stakeholders should also know how long the review process typically takes and be able to identify the appropriate signatories (i.e., official titles) to the contemplated ISAA, if these have not been affirmatively delegated responsibilities. It is important that the stakeholder move in tandem throughout the comment, adjudication, and approval process (i.e.,

[10] *Id*. at § 485(b)(2)(H) and (I).

[11] This paper focuses largely on the bi-lateral arrangement. Looking ahead, multilateral agreements (i.e., many to many), may require consideration of additional factors associated with cross-organization agreements.

[12] This is usually the data custodian or manager of the system that contains the requested information.

[13] For example, early in the planning stage, stakeholders should engage experts in the technical side of the information exchange process when there is greater opportunity to identify technical limitations that may impact sharing options that are under consideration in the ISAA.

that all comments are fully adjudicated before each agreement participant moves to the next round of comments).

B. Develop Your Concept for the Initiative

Stakeholders should participate in the development of the concept for the ISAA. They should allot an appropriate amount of time to lay the groundwork for the initiative to ensure that stakeholders understand the objectives of the information sharing initiative, the provenance and context of the data, any limitations on dissemination, and the intended method for sharing or aggregating the information. This preliminary work will streamline the ISAA development process, improve mission effectiveness, and enable P/CRCL professionals to analyze potential P/CRCL issues and mitigate identified risks.

1. What Are the Specific Purposes of the Information Sharing Initiative?[14]

Understanding the intended purpose of the information sharing initiative is a bedrock P/CRCL requirement, but it is also critical for legal and operational purposes. Representatives of the requesting agency need to describe with some specificity the intended purposes for which the information is requested and the role of the requested information in achieving those purposes. In addition, the purpose of the initiative must tie into the underlying mission of the requesting agency and its enabling authority.

Detail regarding the intended purpose and the specific program the data is intended to be used in is critical to conducting a P/CRCL analysis. Privacy analysis is calibrated on the purposes for which the information will be used; without such information, privacy professionals cannot determine whether the sharing initiative is legally permissible or whether the use of the information is consistent with applicable privacy policies. Potential civil rights and civil liberties impacts may depend on the role of information within an agency's program; information that may be sufficiently vetted for one purpose may present serious civil liberties impacts if used in another. For example, consider information regarding an individual's race or national origin originally collected by an agency for participation in a government benefits program requested for use by a law enforcement agency to map the presence of individuals of a particular race or national origin within its area of responsibility; one may be necessary to identify beneficiaries while the other may present serious civil liberties concerns.

P/CRCL professionals analyze potential P/CRCL impacts to ensure that any such impacts are commensurate with the intended purpose and identify safeguards that may mitigate such impacts. For example, consider the following stated use cases: "to support law enforcement" versus "to be used by background investigators in our security division to vet screening personnel who will be employed by law enforcement agencies." Although both purposes convey an idea of

[14] The term *initiative* includes everything from a multiparty aggregation system to a bilateral information exchange.

intended use (e.g., law enforcement), only the second example provides enough information to assess potential P/CRCL impacts (e.g., false positives or other data quality concerns).

Representatives of the requesting agency should identify all of the intended uses and users of the information during the initial negotiations. Appropriately drafted ISAAs limit the uses and categories of users of the information shared. This is especially significant when the information shared has not yet been identified as terrorism information; the receiving agency cannot use the information for purposes other than those identified in the ISAA. If the intended uses are not identified in the ISAA, parties may seek to amend the existing agreement in order to provide for new uses or users.

2. Who Are the Intended Users?

Closely related to the above, stakeholders need to have a sufficient understanding of who, functionally, within the receiving agency will be using the information. This information assists stakeholders in determining whether the receiving agency is authorized to obtain and use the information. For example, authority to access or use certain types of data may be limited to those components, elements, or individuals within an agency that perform a particular function or operation or may be limited to categories of individuals with certain qualifications or status.

Privacy professionals also may need to understand the purpose for and authority under which the information was collected by the providing agency in order to analyze the appropriateness of the receiving agency's authority to and anticipated use of the information. To the extent that the Privacy Act is applicable, the providing agency is not permitted to share Privacy Act-covered records with the receiving agency unless there is a statutory provision to share the information (this concept is explored in more detail in Section V). Gathering the privacy documentation for the system(s) of records in which the requested information resides, including the System of Records Notice (SORN) and any related Privacy Impact Assessments (PIAs), will assist in making these determinations.

In addition, stakeholders should identify what system of records the shared information will be incorporated into at the receiving agency if the Privacy Act is applicable. In most instances, the information sharing initiative will call for the shared information to be integrated into an existing system or systems of records at the receiving agency. Stakeholders must determine whether the published destination system of records describes as "covered" the type of information that is intended to be shared; if not, either the sharing request must be denied or the SORN updated, as appropriate. For example, if the "destination" system of records provides that the system contains only terrorism information, the receiving agency cannot import a dataset that contains both terrorism and nonterrorism information into that system unless the destination SORN is updated to reflect the new content. If the intended use of the information is beyond the scope of the providing agency's routine use, then the providing agency should consider whether sharing is appropriate. If not, either the sharing request must be denied, or alternatively, the parties' SORNs could be updated, as appropriate, to accommodate the sharing.

3. What Data Is to Be Shared or Aggregated?

The stakeholders should gather key facts regarding the information to be shared or aggregated, including (1) the type of information sought, including its sensitivity; (2) the source and context of the information; (3) the accuracy of the information; and (4) the types of safeguards currently applied to the data, if any (e.g., encryption, anonymization, presearch authorizations and restrictions, additional limits on user accesses, additional audit and monitoring requirements, additional authorizations/preapprovals prior to disseminations). With this information at hand, P/CRCL professionals will then be equipped to assess the potential impact on individuals and to devise protections to mitigate the potential risks associated with the sharing and use of the information.[15]

a. Type of Information

A crucial step in developing a concept for the initiative is understanding the type of information sought and the sensitivity of information contained within. As a threshold matter, the stakeholders should determine whether some or all of the information is PII.[16] In general, datasets containing PII will be subject to more stringent safeguards and sharing limitations than those containing non-PII. Furthermore, the degree of sensitivity of the PII will inform the safeguard and sharing limitations. Some types of PII are more sensitive than other types of PII. For example, a name and phone number on a business card are not considered to be as sensitive as a social security number or a passport number. This type of PII, sometimes called "Sensitive PII," is PII that, if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Sensitive PII requires stricter handling guidelines because of the increased risk to an individual if it is compromised.

If the dataset or system contains PII, stakeholders should also determine whether the information is Protected Information (i.e., subject to protection under executive order, statute, regulation, policy, or other regime). Of relevance to the IC is whether the information is about "United States persons" (USPER) as defined in Executive Order 12333.[17] If a dataset or system contains both USPER and non-U.S. person (non-USPER) information, stakeholders should work

[15] If there is an existing PIA, the PIA would provide some of this information for stakeholders.

[16] See Safeguarding Against and Responding to the Breach of Personally Identifiable Information, OMB Memorandum M-07-16 (May 22, 2007); see also the ISE Privacy Guidelines Glossary, at http://www.ise.gov/sites/default/files/ISEprivacyGlossary.pdf, adopting the definition of PII in M-07-16. PII has several definitions used by federal and state governments as well private sector mission partners. This Framework uses the definition found in OMB M-07-16.

[17] Executive Order 12333 may be found at http://www.archives.gov/federal-register/codification/executive-order/12333.html.

with the policy and technical stakeholders for that dataset/system to determine whether individual records contain accurate indications of USPER status.[18]

In addition to the safeguards generally required for PII, USPER, and Protected Information, certain types of information require heightened vigilance because the nature of the information or the manner in and purpose for which the information is acquired, retained, and used by ISE participants is more likely to impact the P/CRCL of individuals. Stakeholders must determine whether the requested dataset/system contains information that may implicate an individual's constitutional rights and liberties under the First, Fourth, Fifth, and Fourteenth Amendments or other statutory or unenumerated rights or whether the proposed use of the PII contained in the requested dataset/system may have an impact on those rights and liberties.[19] Stakeholders should bear in mind that even when the PII is not about U.S. citizens, some constitutional rights and liberties may still be implicated. For example, First Amendment freedoms are generally available to every person present in the United States, regardless of whether he or she is a U.S. citizen, an LPR, or a visitor.

There may be additional limitations on sharing information. Certain types of information are protected by statute or regulation, regardless of an individual's USPER status. The restrictions may include limits on the agencies the providing agency may share with or the purposes for which the information may be shared; these limits may apply even if the information is terrorism information. Examples of such restrictions include information protected by the Violence Against Women Act, grand jury information protected by the Federal Rules of Criminal Procedure, information protected by the Foreign Intelligence Surveillance Act, and tax return information under the Internal Revenue Code. Other types of information may be similarly restricted by agency policy for a variety of reasons, such as operational security or risk of harm to an individual. Gathering the relevant statutes, regulations, and policies on the types of information requested, in coordination with the providing agency's office of general counsel, will assist the stakeholders in determining whether there are any restrictions the stakeholders should be aware of before drafting the ISAA.

For these reasons, early and ongoing consultation with all of the stakeholders, including the P/CRCL stakeholders and the office of general counsel, focusing on identifying and understanding

[18] Appropriate protections for data will vary based on the type of information and methods available for segregating that information. For example, if accurate, reliable indicators of USPER status are contained in dataset or the parties otherwise have accurate, reliable means of separating the USPER portions of the dataset from the non-USPER portions, it may be possible to deliver the dataset in two segregated sections, to which different sets of appropriate protections may be applied. If, however, USPER information cannot be accurately and reliably separated from non-USPER information, the entire dataset must be protected as if it were USPER information.

[19] Appendix C to this Framework identifies in greater detail the different types of information sensitivity, provides examples of such information and the way P/CRCL issues may arise in the ISE, and identifies considerations for stakeholders in terms of ensuring the proper protection of the information.

the requested information's content and sensitivity will avoid unnecessary delays and ensure that appropriate P/CRCL, technical, and security protections are in place.[20]

b. Source and Context of the Data

Stakeholders need to understand the source and context of the data to be shared. Was the requested data collected by an IC element or by a non-IC, nondefense agency? Was the data collected for law enforcement or intelligence purposes or civil administration? Are the specific data elements of the information requested compulsory or voluntary? If compulsory, is provision of the information mandatory to exercise a constitutional right or receive a government benefit? Specifically, stakeholders should be able to explain how the information was collected, for what purpose, whether it is raw or analyzed,[21] whether there are potential operational sensitivities,[22] and whether the information constitutes terrorism information. It is important to obtain the answers to these questions as a first step because those answers will impact the P/CRCL professionals' assessment of whether the accuracy of the data is sufficient to support its intended use and what type of safeguards may be appropriate.

Sharing With the Intelligence Community (IC)

When an initiative contemplates sharing of information held by a non-IC agency with an element of the IC, stakeholders should recognize that an IC element's receipt of information does not necessarily mean that the element can retain that information for its use. IC elements may retain information about U.S. persons only when the information is of a type authorized by EO 12333 (Section 2.3) and only in accordance with any applicable AG-approved Guidelines implementing EO 12333.

Because datasets held by non-IC agencies are unlikely to contain exclusively terrorism information or other categories of national security information that EO 12333 contemplates, non-IC agencies should be aware that IC elements' AG Guidelines generally authorize a period of assessment within which to determine whether the information received meets applicable criteria for collection and retention (e.g., relevance to mission, category of data). Thus, it is important to consider, in particular, how the information

[20] Understanding the type of information sensitivity will also impact the appropriate sensitivity or classification level of the information to be shared or aggregated (e.g., controlled but unclassified) and inform decisions regarding the technical and security measures appropriate for this level of sensitivity.

[21] Understanding whether the data in question is raw or analyzed may determine the types of protection needed. For instance, raw data may need to be independently verified by the receiving agency before a determination can be made based on the data. With respect to analyzed data, opinions should be clearly identified and recipients should be advised if the records are of questionable accuracy or have known limits on their accuracy.

[22] Identifying operational sensitivities is key to being able to determine whether those who are entitled to protections will in fact be appropriately protected.

may be protected during any such assessment period based on the specifics of that element's AG Guidelines and the specific program or activity involved.

Accordingly, when sharing datasets that do not exclusively consist of terrorism information or other national security information under EO 12333, agencies should take particular care to consider how the IC element's AG Guidelines apply to such sharing. In particular, developing ISAA terms and conditions in such contexts requires recognition of the legal, policy, and operational constraints on the IC participant's receipt and retention of the information shared with it. Therefore, appropriate legal counsel and officers responsible for protection of privacy and civil liberties should be engaged to consider how the IC element's AG Guidelines apply to the specific information to be shared and the protocols for such sharing.

c. Accuracy

A key privacy principle is that PII originating in the agency needs to be as accurate, complete, and internally consistent as the agency requirements specify for use in making determinations, given its authorities and mission.[23] In other words, information used by an agency has to be sufficiently accurate for the purpose for which that agency acquires it.

The required degree of accuracy is related to the potential impact on the individual. This analysis must identify the harm, inconvenience, embarrassment, or unfairness to the individual that could result from use of potentially inaccurate information. The greater the potential impact on the individual (e.g., inclusion on watchlist, denial of benefits or liberty), the stronger the safeguards need to be to mitigate for the greater risk posed by inaccurate information. Safeguards include validation across data sources, encryption, anonymization, presearch authorizations and restrictions, additional limits on user accesses, additional audit and monitoring requirements, additional authorizations/preapprovals prior to disseminations). High-impact activities demand rigorous accuracy.

One challenge to keep in mind is that in information sharing initiatives, the level of accuracy required to meet the purposes for which the providing agency collected the information for a given dataset may not be appropriate for the use proposed by the requesting agency for that dataset. Stakeholders should be watchful for these disparities between the accuracy requirements of the providing agency and the receiving agency. When accuracy may start at a lower level and develop over time, such as in the law enforcement investigatory context, the receiving agency should not use the data for a purpose that requires great accuracy without

[23] See ISE Privacy Guidelines § 5(a); Key Issues Guidance on Data Quality, Core Element 1. The data quality principles contained in the ISE Privacy Guidelines incorporate and build upon the data quality requirements of the Privacy Act of 1974.

putting in place additional, appropriate protections to mitigate the potential impact on individuals (e.g., attempting to revalidate information against other agency holdings, labels to notify the recipient of known limitations on reliability or accuracy, verification by the receiving agency, redress procedures related to correction, and agency review).

Stakeholders should also seek information from the receiving agency as to the types of safeguards that are currently applied to the data that would be shared. The parties will need to consider whether the protections can be relied upon in terms of protecting the classes of data that would be shared or aggregated. If protections would be inadequate, then the stakeholders should anticipate further discussion and analysis regarding the types of protections needed to ensure that those who are entitled to protections are in fact protected by the receiving agency.

C. Methods of Sharing or Aggregating

There are several methods by which an agency may share its information. Section 485(b)(2)(C) of IRTPA directs ISE mission partners to make terrorism-related information available "in a form and manner that facilitates its use in analysis, investigations and operations" and subject to "protections for privacy and civil liberties."[24]

Stakeholders should analyze the various methods available for sharing or aggregating the requested information; these methods may include match/no match responses, account access, requests for information, and bulk transfer of extracts or entire datasets. These examples are ordered to reflect a hierarchy of P/CRCL impacts: generally, the lowest impact would be providing match/no match responses to specific queries. Under this arrangement, stakeholders may be reasonably assured that the data is as up to date as possible and that the providing agency is providing only the data required to meet the recipient agency's mission need. In contrast, the use of bulk transfers presents the greatest potential P/CRCL impact on individuals. With a bulk transfer, the providing agency makes a copy of all the information in its system; depending on the technical capabilities of the partner and specific data sharing arrangement, this may involve some lag between record updates (which typically increases the chance that the information is inaccurate or out of date). Whenever data is exposed to more people, there is an increased chance that data may be lost, stolen, corrupted, or compromised. Similarly, the risks increase with each dataset replication. With bulk transfer, it is frequently more difficult for providing agencies to determine whether the users and uses of the data are consistent with the uses agreed to in the ISAA and to ensure that any updates or corrections to the data are appropriately made. While such concerns may be mitigated by incorporating audit, oversight, and reporting requirements in the ISAA (see Section V.A.6), using a less P/CRCL-impactful method of data sharing is preferable to attempting to mitigate more P/CRCL-impactful methods.[25]

---

[24] *Id.* § 485(b)(2)(H).

[25] For in-depth consideration of the benefits and risks of big data and bulk transfer, see *Big Data and Privacy: A Technological Perspective*, prepared by the President's Council of Advisors on Science and Technology (May 1, 2014), and *Big Data: Seizing Opportunities, Preserving Values*, prepared by a working group led by Counselor to the President John Podesta (May 1, 2014).

When the dataset does not exclusively consist of terrorism information, there is additional sensitivity with regard to bulk sharing of the data outside of the agency that collected it. Before agreeing to bulk sharing of such data with other agencies, agencies should explore whether there are other means for satisfying mission need, such as providing individual account-based access to the native system of the data provider. If, however, the determination is made that bulk sharing is necessary to meet mission need, then additional safeguards, audits, and oversight mechanisms beyond those normally applied may be appropriate to protect the data and to ensure proper oversight and accountability for the data once transferred.

In making the determination as to which method of information sharing is most appropriate for a given circumstance, stakeholders need to consider the information they have gathered thus far regarding the proposed initiative:

- What is the nature of the data to be shared (e.g., USPER vs. non-USPER, terrorism information vs. non-terrorism information, accuracy and reliability, sensitivity of the fields, purposes for which the information was collected)?
- How would the data be used in the requesting agency's particular programs/activities?
- What role, if any, would the receiving agency play in the providing agency's review or use of the data (e.g., would the receiving agency support one of the providing agency's particular mission uses, such as screening)?
- What safeguards are currently applied to the data by the providing agency?
- How will the stakeholders ensure that corrections are consistently applied?

Ensuring the technical feasibility and potential costs associated with the various types of sharing methods considered is critical. Stakeholders will need to provide a clear description of the technical environments of the providing agency and receiving agency. Factors to consider include the data exchange method for delivering the data (e.g., extract transfer load, manual or electronic transfer to a secure FTP server). If manual transfer is planned, then the stakeholders should consider how the data gets written to DVDs and delivered to the receiving agency, including desired frequency. They should also consider how the transfer of data will be tracked and how these metrics will be verified (e.g., ensuring that data recipient records agree with data provider's counts). Finally, stakeholders should consider the encryption method and process that should be used, identifying the tools, uses, and the process for providing encryption keys. Some types of datasets are not always available in each of the sharing methods described above. In addition, the desired outputs of the sharing initiative (discussed below) may affect which method of sharing should be selected.

D. Desired Outputs

In order to properly assess the potential impact of the initiative on P/CRCL, stakeholders should consider how the receiving agency would like to view and use the shared data. What type of reports or query results does the recipient intend to produce? Does the shared data need to be reformatted or aggregated with other data? Does the receiving agency need all of the data elements of individual records or only a subset? For instance, the requesting agency may decide that it needs a report that will produce every piece of information that is tagged to a certain identity or nonobvious relationship or, alternatively, one that generates a map or a graph. With respect to this decision, it is important for stakeholders to consider whether the outputs themselves would be saved. If so, it is likely that the new data formats or aggregated information will require additional analysis with regard to the potential impact on P/CRCL or additional safeguards or oversight measures.

Data that is not particularly sensitive on its own may become very sensitive if it is aggregated with additional information; aggregation may trigger classification requirements or legal- or policy-based additional safeguarding or sharing restrictions. This may be the case even when PII is removed or masked.

Mapping Data

It is not uncommon for a receiving agency to want to map individual or incident data across the agency's area of responsibility. However, even if the PII is removed or masked, significant civil rights and civil liberties concerns may be raised if the data is mapped based on categories that trigger heightened scrutiny, such as race, religion, or national origin. Stakeholders should always ask whether this is an intended output for the shared data, and agencies should consult with their civil liberties advisors and legal counsel in developing the project and ensuring that appropriate safeguards are included in the ISAA and program concept of operations.

E. Appropriate Safeguards

For all types of ISAAs, stakeholders should consider the oversight safeguards that appropriately facilitate the management of the data while ensuring compliance with P/CRCL requirements. Considering the type and sensitivity of data to be shared (e.g., USPER vs. non-USPER), the method of sharing (e.g., account access vs. bulk data), proposed uses, and desired outputs and actions that may be taken on the basis of the shared information, stakeholders should consider the range of safeguards and consultation requirements. For example, the more onward dissemination that is allowed in the agreement, the more auditing and accountability mechanisms the providing agency should consider requiring.

Some types of safeguards and related information an ISAA should include are:

- Applicable authorities for providing the information to the external recipient.
- Applicable authorities for the recipient to receive the information.
- Compliance with both providing agency and receiving agency privacy documentation, including PIAs and SORNs, if applicable.
- Safeguards that implement the FIPPs, to the extent applicable.
- Data breach notification procedures.
- Specified retention periods that are no longer than necessary.
- Procedures for correcting faulty data and providing redress.
- Technical, administrative, and physical security safeguard details.
- Agreement termination dates and procedures.
- Acknowledgement that the parties are members of the ISE and that the parties' collection, use, maintenance, and dissemination of PII under the agreement are consistent with each agency's written P/CL protection policy.
- Designation of the entity or entities that will maintain original signed copies of the agreement and its appendices.
- Point-of-contact (i.e., position vice name) that is responsible for handling administrative activities related to the agreement.

Other types of safeguards and measures that may be appropriate include:

- Auditing terms to ensure compliance with the ISAA under consideration (e.g., audit logs, monitoring for anomalies in the system).
- Providing completed incident reviews to the providing agency.
- PII masking (i.e., depersonalization of data).
- Active/dormant data states.[26]

[26] "Active/dormant data states" refers to a practice of applying additional safeguards to older data that is, due to its age, less likely to be accurate, helpful, or appropriate to share or should be shared less broadly. In this safeguard, data would go "dormant" after a predetermined time period. For example, depending on the content and sensitivity of a particular dataset, analysts should be given general access to the data when it is first collected whenever the analyst has an appropriate predicate to access the data, but after a certain period of years, it would be appropriate to move the data to a physically or logically separated enclave where the data may be accessed only by a more restricted group of personnel than those authorized during the active state or cannot be accessed without a higher level of approval (for example, senior leadership approval) or a more specific purpose than those generally authorized in the active state (for example, for Known or Suspected Terrorist (KST) data extraction only or for searches against specific derogatory information only).

- The process for and frequency of oversight or review meetings (e.g., quarterly, yearly).
- Dissemination limitations, especially where information has not yet been determined to constitute terrorism information.
- Data marking provisions to facilitate redress and coordinate operations.
- Training for handling of sensitive information, especially when the agency does not typically deal with that type of sensitive information (e.g., refugee information).
- Escalation procedures related to the scope of the agreement, interpretation of its provisions, unanticipated technical matters, and other proposed modifications.

In particular, stakeholders should consider what limitations on dissemination are appropriate and necessary. As noted in Section III.B.3, it is important to understand the nature of the information intended to be shared, since certain types of information are protected by statute, regulation, or policy. The restrictions may include limits on the agencies with whom the providing agency may share; law or policy may limit the ability of the receiving agency to receive that data or to share that data with a third-party agency. Stakeholders should examine the relevant statutes, regulations, and agency policies for such restrictions.[27]

In addition to specific dataset or data-type restrictions, the "third-agency rule" generally requires the receiving agency to seek the approval of the providing agency before releasing shared information to a third agency. Executive Order 13526 has generally eliminated the "third-agency rule" as a requirement with regard to information classified after June 28, 2010, unless the sharing agencies take steps to institute the requirement.[28] However, ISAAs should specifically address whether the receiving agency may disseminate shared information without the providing agency's prior approval and, if so, what type of shared information may be disseminated. Provisions restricting third-party dissemination are especially important when the information to be shared is Protected Information and has not yet been determined to constitute terrorism information or other national security information; the ISAA should address whether receiving agencies are permitted to share with third parties information that has not yet been determined to be properly within the ISE, what types of information might be appropriate to share, and what restrictions, if any, should apply. For example, in order to ensure that information flows through the ISE as swiftly as possible, it may be appropriate to permit the receiving agency to share what

[27] Going forward, legal and policy restrictions on access to and dissemination of data may be implemented through such means data tagging.

[28] See Executive Order 13526 § 4.1(i) (Jan. 5, 2010); "Classified information originating in one agency may be disseminated to another agency or U.S. entity by any agency to which it has been made available without the consent of the originating agency[] as long as the criteria for access under section 4.1(a) of this order are met, unless the originating agency has determined that prior authorization is required for such dissemination and has marked or indicated such requirement on the medium containing the classified information in accordance with implementing directives issued pursuant to this order."

appears to be evidence of a crime or imminent terrorist threat with a third party, notifying the providing agency after the sharing. However, it would not generally be appropriate for the receiving agency to pass nonderogatory Protected Information to a third party under those circumstances; requests for information should generally be addressed to the providing agency, rather than a second party with whom the providing agency has shared the information.

IV. What Resources Should ISAA Stakeholders Consult or Gather?

ISAA stakeholders should consult or gather a range of resources that will inform the development of an ISAA:

- Both partners' ISE privacy policies, which set forth the mechanisms for implementing ISE Privacy Guidelines protections applicable to Protected Information.[29]
- If they currently exist, information sharing agreements and any relevant interface control document(s)/agreement(s)[30] regarding the data that delineates how the technical exchange of information occurs.[31]
- Current PIA (if applicable) or SORNs for the data (if applicable).[32]

---

[29] Each ISE department and agency has developed and implemented an ISE privacy policy that is tailored to its respective legal authorities and mission requirements. Stakeholders should refer to their respective department or agency's Web site for a copy of their ISE privacy policy.

[30] Some agencies refer to these agreements as "interconnection agreements."

[31] These documents may be located in the agency's ISAA library, or they may be maintained by the data architect for the system.

[32] In most cases, a SORN and a PIA will both be required when many information technology (IT) systems that collect PII (requiring a PIA) can also retrieve by personal identifier (requiring a SORN); however, in some cases, only a PIA will be required.

The E-Government Act requires agencies to conduct a PIA before (1) developing or procuring IT systems or projects that collect, maintain, or disseminate information in identifiable form from or about members of the public or (2) initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for ten or more persons (excluding agencies, instrumentalities, or employees of the federal government). See Office of Management and Budget Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 26, 2003), at http://www.whitehouse.gov/omb/memoranda_m03-22; E-Government Act of 2002, Pub. L. No. 107-347 (Dec. 17, 2002). According to OMB M-03-22, a PIA "is an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks." In complying with this requirement, P/CL officers use the FIPPs to assess and mitigate any impact on an individual's privacy.

There are some circumstances, however, under which a PIA is not required. See OMB M-03-22 (II)(C). For instance, no PIA is required for national security systems defined at 40 U.S.C. § 11103 as exempt from the definition of information technology. See OMB M-03-22 (II)(C)(3) citing Section 202(i) of the E-Government Act.

In comparison with a PIA, a SORN is required when the agency has a *system of records* as defined by the Privacy Act. The term *record* refers to:

- Applicable treaties or other agreements that apply to the dataset or a subset of information within the dataset (e.g., Terrorism Finance Tracking Program,[33] Passenger Name Record agreement[34]).

- The agencies' statutory and regulatory authorities.

- Any statutes, regulations, or agency policies that relate to sharing or handling of the dataset or subsets of information within the dataset.

- Agency legal guidance and protocols, such as:
  - Executive orders (e.g., EO 12333)
  - For elements of the IC, EO 12333 implementing AG Guidelines and guidance
  - Guidance Regarding Federal Law Enforcement Agencies Regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity (December 2014)[35]
  - Agency information sharing process documents, if they exist

Agencies may employ a variety of methods to obtain much of this information in a single, easy-to-understand format. These include data access request forms, Privacy Threshold Analyses (PTAs),[36] initial privacy assessments, or other processes. However the information is gathered, these resources will help define the contours of contemplated sharing initiative and identify the P/CRCL requirements and policy considerations that stakeholders will need to address in the development and implementation of the agreement.

"[A]ny item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph. . . ."

5 U.S.C. § 552a(a)(4). The term *system of records* refers to "a group of records under the control of any federal agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." *Id.* at § 552a(a)(5). A SORN is a formal notice to the public published in the *Federal Register* that identifies the purpose for which PII is collected, from whom and what type of PII is collected, how the PII is shared externally (routine uses), and how to access and correct any PII maintained by the agency.

[33] See http://www.treasury.gov/resource-center/terrorist-illicit-finance/Terrorist-Finance-Tracking/Pages/tftp.aspx for further information.

[34] This resource may be found at http://www.dhs.gov/xlibrary/assets/privacy/privacy-pnr-agreement.pdf.

[35] This resource may be found at http://www.justice.gov/sites/default/files/ag/pages/attachments/2014/12/08/use-of-race-policy.pdf.

[36] Some agencies may use a PTA to identify programs and systems that are privacy-sensitive, demonstrate the inclusion of privacy considerations during the review of a program or system, provide a record of the program or system and its privacy requirements at the Department's Privacy Office, and demonstrate compliance with privacy laws and regulations. Because an ISAA may be developed concurrently with a PIA, a PTA may provide useful background information on an information sharing effort while the PIA is in development.

V. What Are Some Common Issues or Roadblocks for Agreements?

This section addresses a broad range of issues related to compliance with applicable laws and guidance as well as legal issues affecting the implementation of the ISAA.

A. Compliance

1. Can the Information Be Released to the Receiving Agency Under the Applicable Privacy Laws, Requirements, and Policies?

One of the ways that the Privacy Act of 1974 provides safeguards against unwarranted invasions of privacy is by restricting the disclosure of records containing PII that are maintained by agencies.[37] In order to determine whether the information sought may be released to the receiving agency, the stakeholders must assess whether the information is, first, subject to the Privacy Act and, second, whether it can be disclosed under written consent or an applicable statutory exception.[38] The Privacy Act's protections apply to records that contain information on "individuals" (i.e., U.S. citizens and LPRs),[39] are maintained by a federal agency in a system of records, and are retrieved by a personal identifier (e.g., a person's name, social security number, medical record number, or other unique identifier). One main exception to the Privacy Act's prohibition on disclosure that would be relevant to sharing initiatives is the routine use exception. A *routine use* means, with respect to the disclosure of a record, the "use of such record for a purpose which is compatible with the purpose for which it was collected."[40] The purpose of a routine use is to ensure that agencies have contemplated their external disclosures

---

[37] Conditions of disclosure are set forth in Section 552a(b) of the Privacy Act, which states, in pertinent part, that:

> "No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be—
>
> (3) for a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D) of this section; or . . .
>
> (7) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought. . . ."

[38] See 5 U.S.C. § 552a(b).

[39] See 5 U.S.C. § 552a(a)(2).

[40] 5 U.S.C. § 552a(a)(7). Routine uses apply to information sharing external to an agency. OMB, *Privacy Act Implementation, Guidelines and Responsibilities*, 40 F.R. 28962 (July 9, 1975). OMB, *Privacy Act Implementation, Guidelines and Responsibilities*, 40 F.R. 28953 (July 9, 1975). Common routine uses for most systems of records include sharing (1) for audits and oversight; (2) for congressional inquiries; (3) to contractors, grantees, and experts to perform authorized activities of an agency; (4) for investigations of potential violations of law; (5) for intelligence purposes; (6) to the National Archives and Records Administration for records management purposes; (7) for litigation purposes; and (8) for data breach and mitigation response. See http://www.dhs.gov/xlibrary/assets/privacy/privacy_guidance_sorn.pdf.

appropriate for its mission purposes prior to relying on them, and the Privacy Act requires agencies to provide notice of such routine uses in the *Federal Register*, so that the public receives adequate notice of the agency's purpose(s) for collecting and using their PII.

Stakeholders must analyze the routine uses for the system to determine whether the proposed sharing with a particular partner for a particular purpose is appropriate. The question of whether sharing is covered under a routine use may come down to an interpretation of the breadth of a particular routine use. By way of example, consider a routine use that allows for sharing of information for counterterrorism purposes. Does this mean sharing information for counterterrorism purposes via bulk dissemination, sharing on a case-by-case basis upon request by an agency, or sharing only when there is a specific, identifiable counterterrorism threat? Privacy officials and legal counsel will be key to assisting stakeholders in determining whether the routine use permits the disclosure of the information or, alternatively, whether the routine use can or should be amended. Assuming that the proper procedures for amendment are followed, information maintained in a system of records may be shared under a newly crafted routine use, even when the routine use was published after the record was originally collected by the system. The applicable PIA may also need to be amended if the initiative would necessitate major changes that create new privacy risks.[41] Agencies may also choose to update a PIA to provide additional transparency. For example, although a PIA may already discuss bulk sharing for counterterrorism purposes, an agency may choose to update a PIA to reflect new ISAAs that have been signed. The release of these PIAs may be especially important for agencies that collect large amounts of information from the public. Finally, if an existing collection of

[41] OMB M-03-22 requires PIAs to be performed and updated under the following circumstances:

- *Conversions*—when converting paper-based records to electronic systems.
- *Anonymous to Non-Anonymous*—when functions applied to an existing information collection change anonymous information into information in identifiable form.
- *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.
- *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.
- *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.
- *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).
- *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.
- *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.
- *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).

information with a completed PIA updates or changes its technology, even if the scope of the information collection remains the same, the information collection system should be reviewed in order to analyze whether any new privacy impacts of the technology have been created and whether the PIA should be updated or amended. The SORN covering the system must also be reviewed to ensure its continuing completeness and accuracy but may not necessarily need to be updated.

2. Does the Maintenance of the Data Support the Parties' Missions?

Across the ISE, agencies collect, maintain, and use information pursuant to their varied legal authorities in the performance of a wide variety of missions. Under the Privacy Act, unless an exemption applies,[42] "an agency shall maintain in its system of records only such information as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President."[43] It is important to ensure that both parties' maintenance of the information support their own mission.

It also means that stakeholders should ask themselves whether less information (or less sensitive information) could accomplish the same result. For example, if the receiving agency requires only a portion of the information in a record, that information should be identified and made available and the rest of the information redacted or otherwise segregated so that it is not provided to the receiving agency. As noted in Section III.C, stakeholders should collaborate to determine what data elements are necessary to support the parties' mission and whether other data elements may be excluded.

3. Is the Proposed Sharing Consistent With the Original Purpose of the Collection?

Under the Privacy Act, unless an exemption applies, agencies must provide a statement (a.k.a. "Privacy Act Statement") when collecting information from individuals on the form or the Web site or other location where the information is collected, in order for later sharing to be consistent with the original purpose of the collection. This statement provides notice to all persons who provide PII about themselves that the information will be stored in accordance with Privacy Act requirements and will be shared only in a manner consistent with Privacy Act limitations.[44] This statement must include:

---

[42] The Privacy Act prescribes the circumstances when an agency head can exempt a system of records from certain requirements of the act. See generally 5 U.S.C. § 552a(j), (k). To invoke exemption, the agency must conduct a formal notice and comment rulemaking, and the exemption must be referenced in the appropriate SORN. An agency may not rely on a Privacy Act exemption until the rulemaking is final.

[43] 5 U.S.C. § 552A(E)(1). Agencies can derive authority to collect information about individuals from the Constitution, a statute, or an executive order explicitly authorizing or directing the maintenance of a system of records; or from the Constitution, a statute, or an executive order authorizing or directing the agency to perform a function, the discharging of which requires the maintenance of a system of records. See OMB, Privacy Act Implementation Guidance, at 28960, at http://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/implementation_guidelines.pdf.

[44] 5 U.S.C. § 552a(e)(3).

- The legal authority for collecting the information (e.g., statute, executive order, regulation).
- The purposes for collecting the information and how the agency will use it.
- The routine uses that may be made of the information (i.e., to whom the providing agency may disclose the information outside the agency and for what purposes).
- The effects on the individual, if any, of not providing the requested information (e.g., denial of benefits).

The stakeholders should also consider whether there are policy reasons why this information should not be used in a data aggregation system or made available to a particular user. For example, while the Privacy Act does not constrain agencies in the sharing of records about non-U.S. citizens/non-LPRs, some agencies extend Privacy Act sharing limitations to all individuals, regardless of immigration or citizenship status. Stakeholders should be mindful that this mixed systems policy limits the sharing of non-USPER information, similar to USPER information.

4. How Long Should the Information Be Retained?

In regard to information shared among agencies, there are two types of retention. A retention period may be set through negotiation between the agencies, especially when records have not yet been determined to be relevant to the recipient's needs or may be determined by Privacy Act principles and administrative determinations. This latter type of retention ensures compliance with the Federal Records Act (FRA) and Records Control Schedules (RCS). If the ISAA does not permit the receiving agency to modify or control the providing agency's information, the information is treated as a "reference copy" available for the recipient's consultation. However, if the ISAA does permit the receiving agency to modify or control the providing element's information, this may result in a "new record" (i.e., the original record is used in a product, added to or changed in any way, or permanently incorporated into a receiving agency system of records); then the new record is governed by the RCS of the agency that created the new record. As noted in Section III.E, specific periods for retaining (using) the reference copies shared under the initiative should be set out in the ISAA, including the agreed-upon start and end dates. Appropriate retention periods vary based on the reasons for which the data is being shared, the type and sensitivity of the data shared, the method of sharing, and the authorities of the parties.

The first principle of establishing an appropriate retention period is that the data should not be retained for longer than required to fulfill the use for which the data is being shared. Stakeholders should also note whether there is a law, a regulation, or a policy that sets an outside limit for retention of the data or some subset of the data, e.g., special restrictions on the retention of information regarding refugees.

Retention limits are an important privacy protection that, like all privacy protections, should be driven by the FIPPs, as applicable. Stakeholders should also note the length of time the providing

agency retains the data in its system of records. It should not be assumed that the receiving agency necessitates the same retention period as that of the providing agency. Other policy or FIPPs considerations may establish a more restrictive retention period than what is legally permissible.

When a sharing initiative involves the providing agency sharing information so the receiving agency may make a determination as to whether the information is relevant to its mission needs, the retention section of the ISAA should specifically address how long the receiving agency may take to make that determination, how long it may retain the data relevant to its mission, and how it must dispose of the information that is not relevant to the mission. For example, when a non-IC agency shares data with an element of the IC so that the IC element may determine whether the information falls into one of its collection authorities, the ISAA should include a timetable for the collection decision and the disposition of data that is not retained. Even if the IC element's EO 12333 implementing guidance sets an absolute outward limit on the amount of time the element has to decide whether to retain the data, shorter periods may be appropriate based on the nature of data being shared (e.g., the circumstances under which it was collected by the providing agency, the sensitivity of the fields requested, the degree of USPER content, and the mission benefits).

In any case, the receiving agency should make clear to the providing agency why the receiving agency needs the time it has requested to make a determination as to whether the information is relevant to its mission needs, so the providing agency may assist in determining the appropriate period for making the determination and the providing agency may amend its privacy documentation to disclose to the public the drivers behind the temporary retention of the data. For example, is the length of the period provided for making a determination as to whether the information is relevant to the receiving agency's mission need related to the average time it takes to conduct an analysis of the records provided, or are other facts also considered? The receiving agency should make clear whether records will be retained for varying lengths of time based on mission, whether all records will be retained in order to create a baseline by which to potentially detect anomalous behavior, or whether it desires to retain all records for the maximum period its authorities permit because of the possibility that at any point in time new information may reveal a previously undetected link to its mission need.

5. What Are the Notification Requirements Should There Be a Data Breach?

The ISE P/CRCL protection framework depends upon responsible sharing and safeguarding of terrorism-related information. Safeguarding PII in the possession of the government and preventing its breach are essential to ensure that the government retains the trust of the American public.

Federal departments and agencies are required to develop and implement a breach notification policy (a.k.a. "information incident" or "privacy incident")[45] and must report to the United States Computer Emergency Readiness Team (US-CERT) when there has been unauthorized access or any suspected or confirmed breach of PII.[46] Such reporting is required within one hour of discovery/detection.

As noted in Section III.E, data breach procedures should be included in all ISAAs. The ISAA should address not only the data breach notification requirements that will apply to the initiative but also whose breach notification policy controls. With respect to the notification requirements, the parties should address the timing required for the notification (e.g., "receiving agency will notify providing agency within [insert period of time] of the breach"), which agency should receive notification, and how the notification should be made (e.g., e-mail, telephone). It is critical that the ISAA clarify whose policy would control in the event of a breach because the agencies' policies and procedures may be significantly different, especially when the initiative involves IC agencies and non-IC agencies.

6. What Accountability Measures Are Needed?

IRTPA's requirement that the ISE "incorporate strong mechanisms to enhance accountability and facilitate oversight, including audits, authentication, and access controls"[47] raises several considerations for parties to an ISAA with regard to appropriate accountability measures. For instance, the parties should consider whether the agreement should impose a requirement to cooperate in compliance reviews conducted by the other agency or, alternatively, whether the providing agency could obtain a copy of any compliance reviews conducted by the agency holding the data. It is a best practice to exchange accountability information to ensure compliance with applicable laws and ISAA requirements.

As noted in Section III.E, the methods for ensuring accountability will vary, depending on (1) the type of system(s) involved and (2) the sensitivity of the information that will be shared (e.g., statistical analysis used to support high-level policy analysis versus information describing how an individual exercises rights guaranteed by the First Amendment). In general, the restrictiveness of specific safeguards should be commensurate with the potential P/CL impact of the initiative. For example, bulk transfers of information, especially data that has not yet been determined to constitute terrorism or other national security information, should generally be subject to more stringent accountability measures, such as greater restrictions on access to the bulk data and

[45] See OMB M-07-16. This is a responsibility shared by officials accountable for administering operational and privacy and security programs, legal counsel, agencies' Inspectors General and other law enforcement, and public and legislative affairs. It is also a function of applicable laws, such as the Federal Information Security Management Act of 2002 and the Privacy Act. See OMB M-07-16, at 1.

[46] The term *breach* refers to "the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to [PII], whether physical or electronic." See OMB M-07-16.

[47] 6 U.S.C. § 485(2)(2)(I).

more frequent audits/compliance reviews. Stakeholders should also consider the downstream effects of the use of this information on an individual (e.g., individual cannot travel at all versus one in which he or she is delayed in travelling). An analysis of these factors should also inform the stakeholders' decisions in terms of the appropriate parameters of auditing (e.g., internal or external, random or scheduled audits, use of audit logs to provide the capacity to find anomalous use).

7. How Long Should the Agreement Persist?

ISAAs should specify a specific termination date, not to exceed five years from the date the agreement is executed. Even in long-lived sharing arrangements, this will give the parties an opportunity periodically to review the effectiveness of the sharing program; evaluate—particularly in bulk sharing arrangements—whether less privacy-sensitive sharing alternatives exist; amend terms and conditions to reflect evolving civil rights, civil liberties, or privacy standards; or incorporate additional protections measures.

B. Legal

1. To the Extent That the Privacy Act Applies, Whose SORN Applies to the Shared or Aggregated Information?

The question of whose SORN applies to the information, once shared, would depend upon whether the information is "maintained" in a "system of records" for purposes of the Privacy Act.[48] The providing agency's SORN always applies to the initial question of whether the information may be shared; however, as noted in Section III.B.2, the SORN of the receiving agency is often also significant. The parties should reach agreement about which SORN applies to the data at which point in time, and this SORN coverage should be documented in the ISAA. If, for example, the providing agency makes the information available to the requesting agency by providing access to the information (e.g., providing authorized access to its system via a Web-based platform), the providing party's SORN would govern the records in the system (as they remain in the providing agency's system). If, however, the requesting agency receives the information by copying it (or some portion of it) from the Web-based platform and uploads or otherwise transfers the information to its own system of records, the portion of the records actually copied/received will be governed by the requesting agency's SORN as it relates to its maintenance of that record when information is retrieved by users who input a personal identifier. If the information sharing initiative contemplates replication and transfer of records to the receiving agency (e.g., through bulk transfer), stakeholders must determine whether the destination system of records appropriately reflects that it covers the type of information that is intended to be shared.[49] If a collaborative environment is planned (i.e., several agencies are

[48] For the definitions of *record* and *system of record*, refer to Footnote 32 of this Framework.

[49] Once the information is received, the recipient's SORN applies to any subsequent external sharing and the stakeholders may, by agreement, restrict onward external disclosures that the receiving party's SORN would otherwise permit. However, disclosures internal to the receiving entity are permitted by subsection (b)(1) of the

contributing to a shared space), then this is a more complex arrangement, requiring each agency to separately analyze its privacy policy and/or Privacy Act obligations to ensure compliance with applicable statutory and policy requirements. When federal and state, local, and tribal agencies enter into an information sharing relationship, the obligations of the parties vis-à-vis the information should be clearly set forth in the ISAA. Further, a receiving agency that enters into an information sharing relationship should also ensure that it will apply all available exemptions under both the Freedom of Information Act (FOIA) and the Privacy Act, consistent with how the providing agency applies the same exemptions. For example, information originally compiled for law enforcement purposes, even when recompiled into a non-law enforcement record, would not lose its exempt status, and the terms of the ISAA should clearly describe the nature of such information.

2. Who Is Responsible for FOIA/Privacy Act Requests and What Is the Process for Handling?

The FOIA generally gives any person a statutory right to request access to federal agency records.[50] This right to access is limited when information is protected from disclosure by one of FOIA's nine statutory exemptions.[51] A federal agency, for instance, is not required to disclose national security classified information or law enforcement records (to the extent that one of six specific harms could result from disclosure). The Privacy Act also provides individuals with the right to access records pertaining to them maintained by federal agencies. This right may be subject to exemption in certain circumstances, such as for criminal law enforcement and classified records.[52]

The ISAA should describe the arrangement for handling FOIA requests. This provision is needed because individuals seeking access to any record containing information that is part of the agency's system of records or seeking to contest the accuracy of its content may submit a FOIA or Privacy Act request to one of the parties. The parties will need to understand how to coordinate the development of a response and any production of or access to records. The responsibility to process FOIA and Privacy Act requests may be assigned by agreement of the parties. Regardless of who administratively processes the request, in the absence of an arrangement, when information is transferred in bulk from a non-IC agency to an element of the IC, the providing agency typically makes the disclosure determination. Also, given the nature of some of the information shared through the ISE (i.e., sensitive law enforcement or intelligence information), coordination of any response or production of records by the non-IC element with the law enforcement or IC element is essential, so that sensitive investigative, prosecutorial, or intelligence equities are not compromised.

Privacy Act. See 5 U.S.C. § 552a(b)(1). As a matter of policy, secondary internal disclosures are also subject to the restrictions of the ISAA, which may be more restrictive than subsection (b)(1).

[50] See 5 U.S.C. § 552.

[51] *Id*. at § 552(b).

[52] 5 U.S.C. § 552a(d).

3. Obligations in Case of Litigation

The ISAA should clearly delineate the responsibilities of the providing and requesting parties in the event of litigation arising from the information sharing initiative(s).

4. Obligations Vis-à-Vis Applicable Redress Programs

In accordance with Section 8 of the ISE Privacy Guidelines, each agency participating in the ISE, consistent with its legal authorities and mission requirements, is required to provide "redress" (i.e., a procedure for addressing complaints relating to Protected Information in the ISE).[53] The ISE Privacy Guidelines contemplate that agencies will afford redress with respect to issues involving P/CRCL and other legal rights protected by law. Therefore, the ISAA will need to delineate the parties' respective obligations relating to redress, identifying which agency's complaint/review procedures would be used and what the process would be for addressing such complaints (e.g., alleged racial, ethnic, or religious profiling; retention in the ISE of information that has been expunged or determined to have been illegally collected).

The redress procedures contemplated by the ISE Privacy Guidelines, addressed in the parties' respective ISE privacy policies and incorporated by reference into the ISAA, must cover situations involving complaints that implicate Protected Information in the ISE.[54] This would neither alter the agency's rules regarding record access or other rights nor require the responsible party to either acknowledge the existence of records or inform complainants of case status or resolution when no such right currently exists.[55] Because individuals often may not recognize that there is any relationship between the complaint and the ISE, the responsible party must have procedures in place to identify those complaints that are related to Protected Information in the ISE (i.e., Protected Information that originated with the responsible party or was obtained through the ISE). The responsible party must then coordinate with all involved agencies to investigate and correct (or remove) any identified information deficiencies. The process must also ensure that the complaints[56] are brought to the attention of the responsible party's ISE P/CL Official (or designee) in accordance with agency policy.

The ISE Privacy Guidelines protect the P/CRCL of U.S. citizens and LPRs and, for the IC, USPERs as defined in EO 12333. However, these categories of Protected Information may be expanded to include other information that the U.S. government expressly determines by executive order,

---

[53] Section 8 of the ISE Privacy Guidelines provides that:

> To the extent consistent with its legal authorities and mission requirements, each agency shall, with respect to its participation in the development and use of the ISE, put in place internal procedures to address complaints from persons regarding Protected Information about them that is under the agency's control.

[54] That is not to say, however, that the Protected Information would necessarily be under the control of the agency receiving the complaint.

[55] As is true under existing processes, many information privacy, Privacy Act, or CRCL complaints identified as involving Protected Information in the ISE will not result in the complainant being informed of measures the agency takes to investigate a complaint, rectify an alleged error, or remedy an issue.

[56] This is limited only to those complaints implicating Protected Information in the ISE.

international agreement, or other similar instrument shall be covered by the ISE Privacy Guidelines. Indeed, many agencies share Protected Information pursuant to international agreements that allow foreign nationals access to review procedures. When a complaint/review process is required by international agreement, special procedures may be employed for foreign nationals (to the extent that such details are not spelled out in the agreement).

Regardless of which redress program is used, the ISAA should also require the receiving agency to appropriately mark or otherwise be able to track the shared information so that the redress program is effective, and even where no complaint has been made, the providing agency can provide the receiving agency with correction or updates to the data, if appropriate. The ability to identify and correct faulty or out-of-date data is key to providing effective redress. When an ISAA also permits the receiving agency to share with a third agency, the ISAA should include appropriate marking and handling provisions so that the third agency understands the origin of the data and any limitations on its use or concerns regarding its accuracy.

5. Include a Comprehensive List of Definitions

As with any legal document, key words and phrases used in the ISAA must be identified and defined in the agreement.[57] The stakeholders will need to work closely with their P/CL officials, as well as their legal counsel to ensure that key terms are defined in a manner that is consistent with law and accurately reflects the intentions of the parties. This is especially important when the agreements are between elements of the IC and non-IC agencies or entities because the same term may have a number of potential interpretations depending upon the statutory scheme.

A list of defined terms is included in the glossary of the Framework. In addition, stakeholders may refer to the Privacy and Civil Liberties Web page on the U.S. Department of Justice, Office of Justice Programs, Web site.[58] This link defines commonly used terms in privacy, civil liberties, and information sharing using the exact language of various federal statutes, regulations, policy guidance, and other sources.

For the convenience of the stakeholders, the P/CL Subcommittee has also developed a worksheet that reflects the steps and considerations for streamlining the ISAA development process and incorporating P/CRCL best practices. See Attachment D.

VI. Final Steps

Once the appropriate stakeholders have the ISAA in a draft that is amenable to both parties, there are a few remaining ISAA considerations. First, stakeholders need to ensure that they understand the effect of the agreement upon signing. For instance, does the agreement permit

[57] The worksheet addressing core P/CRCL protections will include sample definitions for some of the key terms frequently contained in ISAAs.
[58] See http://www.it.ojp.gov/default.aspx?area=privacy&page=1268.

information to flow once the agreement is signed, or is the agreement actually only a statement of intent to enter into another agreement at some point in the future? In order to be able to begin sharing information pursuant to the agreement, are implementing arrangements or interface control documents[59] needed to set up the technical exchange (e.g., the technical parameters for the data exchange, data dictionary)? It is generally easier to answer these questions if technical stakeholders are involved from the early stages of the contemplated agreement. Second, it is also important for stakeholders to understand how data will be delivered to the receiving agency,[60] how it will be tracked,[61] and how these metrics will be used to determine the extent to which that data recipient's records agree with the data provider's counts; the data provider and receiving agency should have the technical measures to implement the agreement in place before data is shared. In addition, the parties may also wish to recite in the ISAA the caveat that the agreement is intended to improve internal management of the federal government and does not in itself create any enforceable rights or benefits. Finally, the parties should determine whether there is an internal agency repository of ISAAs they need to contact upon signing of the agreement and what, if any, additional internal or external stakeholders should receive a copy of the signed agreement. All stakeholders should be sent a final copy of the agreement.

[59] Some agencies may alternatively refer to such documents as "interconnection agreements."

[60] For example, the data may be delivered via CDs streaming or be placed on a secure Web site.

[61] In other words, the stakeholder should have a way of establishing, for instance, how many records have been delivered to the receiving agency during a defined period of time.

ACRONYMS

AG	Attorney General
DOJ	U.S. Department of Justice
FIPPs	Fair Information Practice Principles (a.k.a. "Fair Information Practices")
FOIA	Freedom of Information Act
EO	Executive Order
IC	Intelligence Community
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
ISAA	Information Sharing and Access Agreement
ISE	Information Sharing Environment
IT	Information Technology
LPR	Lawful Permanent Resident
P/CRCL	Privacy, Civil Rights, and Civil Liberties
P/CL	Privacy and Civil Liberties
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PM-ISE	Program Manager for the ISE
PTA	Privacy Threshold Analysis
SORN	System of Records Notice
US-CERT	United States Computer Emergency Readiness Team
USPER	United States Person
Non-USPER	Non-United States Person

GLOSSARY[62]

Agency – means the term "executive agency" in section 105 of title 5, United States Code, but includes the Postal Rate Commission and the United States Postal Service and excludes the Government Accounting Office. ISE Privacy Guidelines *§13(a)(i).*

Homeland Security Information – means any information possessed by a federal, state, local, or tribal agency that relates to (A) a threat of terrorist activity, (B) the ability to prevent, interdict, or disrupt terrorist activity, (C) the identification or investigation of a suspected terrorist or terrorist organization or any person, group, or entity associated with or assisting a suspected terrorist or terrorist organization, or (D) a planned or actual response to a terrorist act. ISE Privacy Guidelines §13(a)(iii), *as derived from section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. 482(f)(1)).*

Individual – means a citizen of the United States or an alien lawfully admitted for permanent residence. See 5 U.S.C. § 552a (a)(2).

Law Enforcement Information – means any information obtained by or of interest to a law enforcement agency or official that is (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. ISE Privacy Guidelines §13(a)(iii).

Personally Identifiable Information – means any information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. OMB Memorandum M-07-16, May 22, 2007.

Protected Information – means information about U.S. citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and Federal laws of the United States. ISE Privacy Guidelines §1(b). For the 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.

[62] http://www.ise.gov/sites/default/files/ISEprivacyGlossary.pdf.