# Privacy and Civil Liberties Implementation Guide *for the* Information Sharing Environment

**This Implementation Guide has been designed to provide a suggested process to assist Federal departments and agencies in implementing the ISE Privacy Guidelines. It is not intended to be prescriptive, but rather to provide a broad-based process framework and guidance that can be adapted to each agency's unique structure and needs.**

**Version 1.0**

# Overview

*Purpose.* The purpose of this document is to help Federal agencies implement the *Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment* (ISE Privacy Guidelines). Currently, this document provides a framework concentrated on issues at a Federal agency level and not specifically applied for use by nonfederal entities, notably state, local, and tribal entities. Guidance on privacy concerns in the development and operation of state and local fusion centers can be found as Guideline 8 in the *Fusion Center Guidelines*, issued by the U.S. Department of Justice's Global Justice Information Sharing Initiative, in coordination with the U.S. Department of Homeland Security. Nonetheless, this document can provide a useful supplement to that guidance. Additionally, a review of the specific qualifications to implement appropriate policies and procedures that provide privacy protections that are at least as comprehensive as those contained in the ISE Privacy Guidelines on the state, local, and tribal level is currently under development for use by state, local, and tribal entities.

*Background.* In the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Congress established the need to protect privacy and civil liberties as a core tenet of the ISE. In accordance with IRTPA Section 1016(d) and in furtherance of Executive Order 13388, the President of the United States approved for issuance and implementation the ISE Privacy Guidelines. These guidelines provide a framework to enable information sharing while protecting privacy, civil liberties, and other legal rights.[1] Therefore, by Act of Congress and direction of the President, each agency **shall** ensure that the ISE Privacy Guidelines are fully implemented.[2]

*Core Principles and Activities.* The ISE Privacy Guidelines do more than direct agencies to comply with the law.[3] They set forth a set of core privacy and civil liberties principles and activities that agencies will follow. These principles and activities are:

- Identify and review protected information that may be shared via the ISE.
- Enable ISE participants to determine the nature of protected information that may be shared and any applicable legal restrictions.
- Share protected information in the ISE only to the extent it is terrorism related information.[4]

---

1 Program Manager, Information Sharing Environment Memorandum, Subject: *Privacy Guidelines for the Information Sharing Environment*, December 4, 2006. The ISE Privacy Guidelines are attached to this memorandum.

2 Ibid.

3 An Introduction to the ISE Privacy Guidelines, "Compliance With Law," page 2. The ISE Privacy Guidelines and any policy implementing them, however, are intended to improve the internal management of the federal government and are not intended to, and do not create any rights or benefits, substantive or procedural, enforceable at law or inequity by a party against the United States, its departments, agencies, or entities, its officers, employees, or agencies, or any other person. See ISE Privacy Guidelines at 13.d.(iv).

4 In accordance with IRTPA, as recently amended by the 9/11 Commission Act enacted on August 3, 2007 (P.L. 110–53), the ISE facilitates the sharing of terrorism and homeland security information, as defined, respectively, in IRTPA Section 1016(a)(5) and the Homeland Security Act 892(f)(1) (6 U.S.C. §482(f)(1)). See also *Information Sharing Environment Implementation Plan* (November 2006) and Presidential Guidelines 2 and 3 (provided that the ISE would facilitate the sharing of "terrorism information," as then defined in IRTPA, as well as the following categories of information to the extent that they do not otherwise constitute "terrorism information": (1) homeland

- Assess, document, and comply with all applicable laws and policies.
- Establish data accuracy, quality, and retention procedures.
- Deploy adequate security measures to safeguard protected information.
- Implement adequate accountability, enforcement, and audit mechanisms to verify compliance.
- Establish a redress process consistent with legal authorities and mission requirements.
- Implement ISE Privacy Guidelines requirements via appropriate change to business processes and systems, training, and technology.
- Make the public aware of the agency's policies as appropriate.
- Ensure that, in order to share information in the ISE, nonfederal entities—including state, local, tribal, and foreign governments— develop and implement appropriate policies and procedures that provide protections that are at least as comprehensive as those contained in the ISE Privacy Guidelines.
- Designate a senior official accountable for implementation (ISE Privacy Official).

*Required Actions.* Consistent with the authorities to develop, implement, and integrate the ISE, each agency that possesses or uses intelligence or terrorism related information, operates a system in the ISE, or otherwise participates in (or expects to participate) in the ISE must ensure its full compliance with information sharing policies and guidelines that have been established by the President and the Program Manager for the ISE.[5] Pursuant to the ISE Privacy Guidelines to implement the President's Memorandum[6] and IRTPA, each Federal agency shall adopt internal policies and procedures to ensure that the agency accesses and uses protected information in the ISE consistent with the authorized purpose of the ISE.

*Role of the Program Manager.* On April 10, 2007, the President assigned his functions under IRTPA Section 1016(b) to the Director of National Intelligence (DNI), to be performed in a manner consistent with the President's direction and guidance. On May 2, 2007, the DNI delegated his authority to the Program Manager to carry out all of these assigned duties under Section 1016(b). The Program Manager's assigned duties under Section 1016(b) specifically include creating an ISE in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties; designating organizational structures to operate and manage the ISE; and determining and enforcing the policies, directives, and rules that will govern the content and usage of the ISE. The Program Manager's duties, as further described in IRTPA Section 1016(f), include monitoring and assessing the implementation of the ISE by Federal departments and agencies to ensure adequate progress and policy compliance and regularly reporting to Congress. [7]

*Role of the Implementation Guide.* The Implementation Guide describes best practices and a methodology to ensure implementation of the protections and safeguards required by the ISE Privacy Guidelines. The Implementation Guide is not meant to be prescriptive but rather the actual

security information and (2) law enforcement information relating to terrorism or the security of our homeland). Such additional information includes intelligence information.

5 See IRTPA Section 1016(i).

6 December 16, 2005, Memorandum, *Guidelines and Requirements in Support of the Information Sharing Environment.*

7 See IRTPA Section 1016(f)(2)(A)(iv) (as amended by the 9/11 Commission Act of 2007) (identify and resolve information sharing disputes between federal departments, agencies, and components); and Section 1016(h)(2)(I) (report to Congress annually, including an assessment of the privacy and civil liberties protections in the ISE).

process of implementation can be tailored by each agency to fit its unique environment as it implements the ISE Privacy Guidelines. As such, the ISE Privacy Guidelines require each Federal agency to develop and implement a written ISE privacy policy that sets forth the mechanisms, policies, and procedures its personnel will follow in implementing the ISE Privacy Guidelines. Further, to the extent possible, this privacy policy should be written for public release to assist in informing and educating the public in the protections and safeguards employed by each agency to ensure privacy and civil liberties.[8]

*Role of the Privacy Guidelines Committee*. The Program Manager established the Privacy Guidelines Committee (PGC)[9] to provide additional guidance on the implementation of the guidelines, promote consistent interpretations of applicable legal requirements, avoid duplication of effort, share best practices, and provide a forum for resolving issues on an interagency basis. The PGC will provide ongoing guidance on the implementation of the ISE Privacy Guidelines to assist agencies in their ISE privacy and civil liberties protection efforts.

*Role of the Federal Agencies*. Responsibility for the implementation of the ISE Privacy Guidelines through agency policy will fall directly to the individual agencies. As agencies consider how they will approach their implementation of the ISE Privacy Guidelines, they may use their existing processes or may wish to consider using the process suggested herein, in whole or in part, in sequence or in parallel. In addition to each individual Federal agency's internal mechanisms for ensuring compliance with the ISE Privacy Guidelines, the PGC will serve as a forum for resolving interagency issues. To facilitate the PGC's work, each agency will share with the PGC its ISE privacy policy,[10] not for approval purposes, but rather to enable it to better anticipate and resolve interagency issues, ensure that agency policies reflect consistent interpretations of the PGC, and respond to Program Manager requests regarding the status of ISE Privacy Guidelines implementation pursuant to the Program Manager's authorities under IRTPA.

Successful implementation of this effort necessitates that an agency consider how it will govern or oversee the information sharing process and what resources it will require to undertake the implementation of its ISE privacy protection policy. Some agencies may already have an existing governance structure that could be used to implement the ISE Privacy Guidelines. The ISE Privacy Guidelines require each agency to designate a senior official as the ISE privacy official, with overall agencywide responsibility for information privacy issues and for directly overseeing the agency's implementation and compliance with the ISE Privacy Guidelines. It may be useful to create a team that consists of executive-level sponsorship, privacy and civil liberties officers, designated ISE officials, and other information officers, program managers, and legal counsel. Given that this effort cuts across different areas, it may be helpful to have a broad team that is knowledgeable about information sharing, terrorism-related information, and privacy and civil liberties.

Agencies should recognize that the process of implementing the ISE Privacy Guidelines is an iterative process. It may be necessary to reevaluate their privacy policy frameworks and/or how those frameworks are applied to information shared in the ISE if new laws are passed, Executive

[8] An agency privacy policy should be written for release acknowledging the need to protect classified, sensitive, or otherwise privileged information from unauthorized disclosure.

[9] ISE Privacy Guidelines, Section 12.

[10] The PGC will provide separate guidance on when and how to share the privacy policy with the PGC.

Orders are issued, and/or information sharing arrangements and agreements (hereinafter referred to as sharing arrangements) are identified.

# Authority

The authority for the ISE Privacy Guidelines and the requirement for their implementation may be found in the following:

- Intelligence Reform and Terrorism Prevention Act (December 17, 2004)[11]
  - *IRTPA Section 1016(b)(1)(A)*—The President shall create an information sharing environment for the sharing of terrorism information in a manner that is consistent with national security and with applicable legal standards relating to privacy and civil liberties.
  - *IRTPA §1016(b)(1)(C)*—The President shall determine and enforce the policies, directives, and rules that will govern the content and usage of the ISE.
  - *IRTPA §1016(d)(2)(A)*—The President shall in consultation with the Privacy and Civil Liberties Oversight Board established under Section 1061, issue guidelines that protect privacy and civil liberties in the development and use of the ISE.
  - *IRTPA §1016(i)*—The head of each department or agency that possesses or uses intelligence or terrorism information, operates a system in the ISE, or otherwise participates (or expects to participate) in the ISE shall (1) ensure full department or agency compliance with information sharing policies, procedures, guidelines, rules, and standards established under subsection (b) and (f); (2) ensure the provision of adequate resources for systems and activities supporting operation of and participation in the ISE; (3) ensure full department or agency cooperation in the development of the ISE to implement government-wide information sharing; and (4) submit, at the request of the President or the program manager, any reports on the implementation of the requirements of the ISE within such department or agency.
- Executive Order 13388 (October 25, 2005), Further Strengthening the Sharing of Terrorism Information to Protect Americans
  - *§1(b)*—To the maximum extent consistent with applicable law, agencies shall, in the design and use of information systems and in the dissemination of information among agencies . . . protect the freedom, information privacy, and other legal rights of Americans in the conduct of activities implementing subsection (a).
  - *§7(a) (i)*—This order: shall be implemented in a manner consistent with applicable law, including Federal law protecting information privacy and other legal rights of Americans.
  - *§2*—To implement the policy set forth in Section 1 of [EO 13388], the head of each agency that possesses or acquires terrorism information (a) shall promptly give access to the terrorism information to the head of each other agency that has counterterrorism functions, and provide the terrorism information to each such agency, unless otherwise directed by the President, and consistent with (i) the statutory responsibilities of the agencies providing and receiving the information; (ii) any guidance issued by the Attorney General to fulfill the policy set forth in subsection 1(b) of [EO 13388]; and (iii) other applicable law, including Sections 102A(g) and (i) of the National Security Act of 1947, Section 1016 of the IRTPA (including any policies, procedures, guidelines, rules,

[11] Section 1016 of IRTPA was recently amended, in part, by the 9/11 Commission Act, P.L.110–53.

and standards issued pursuant thereto), Sections 202 and 892 of the Homeland Security Act of 2002, EO 12958 . . . and EO 13311 . . . [citations omitted; emphasis added].

- Presidential Memorandum (December 16, 2005)
  - *§2 Information Sharing Guidelines, (e) Guideline 5—Protect the Information Privacy Rights and Other Legal Rights of Americans, (ii),* Each head of an executive department or agency that possesses or uses intelligence or terrorism information shall ensure on an ongoing basis that (A) appropriate personnel, structures, training, and technologies are in place to ensure that terrorism information is shared in a manner that protects the information privacy and other legal rights of Americans, and (B), upon approval by the President of the guidelines developed under the preceding subsection (i), such guidelines are fully implemented in such department or agency.

# Implementation Stages

The ISE Privacy Guidelines provide a framework for (1) identifying information that is subject to privacy protection, (2) assessing applicable privacy rules, (3) implementing appropriate protections, and (4) ensuring compliance.[12] These four broad categories provide the basis for a two-stage implementation process described below.

- Stage I—Identify and Demonstrate the Agency's Privacy Policy Framework for Achieving Compliance With ISE Privacy Guidelines
- Stage II—Application of the Agency's Policy Framework to ISE Information Sharing Arrangements/Resources

Stage I is about law and policy. The ISE Privacy Guidelines **require** that an agency shall develop and implement a written ISE privacy protection policy (ISE Privacy Guidelines, Section 12(d)). To develop this policy, agencies need to determine whether their existing policies already comply with the ISE Privacy Guidelines. There are three steps that will help agencies make this determination: identify, assess, and protect.

- Step 1 is to identify any applicable laws, Executive Orders, policies, and procedures that apply to protected information that the agency will make available or access through the ISE. This will provide the authorities that an agency needs to consider when determining whether its policies comply with the ISE Privacy Guidelines. To comply with the ISE Privacy Guidelines, an agency must follow all applicable laws that apply to protected information, as well as the specific policy requirements set forth in the ISE Privacy Guidelines.
- Step 2 is to assess those identified laws, Executive Orders, policies, and procedures to determine whether they satisfy the requirements of the ISE Privacy Guidelines or whether additional policies are needed to ensure compliance with the Guidelines. If the policies are lacking or are otherwise not in compliance, this step will help determine any gaps in privacy protection.
- Step 3 is to protect by ensuring that all protected information in the ISE is covered by applicable privacy policies. This may be done by documenting the existing policies that comply with the ISE Privacy Guidelines or identifying, where necessary, the need to develop new policies that bring the agency into compliance with the ISE Privacy Guidelines. Once an agency is able to document that its policies are in compliance with the ISE Privacy Guidelines, the agency applies the policies to the systems and sharing arrangements in the ISE. This written ISE Privacy Protection Policy satisfies ISE Privacy Guidelines, Section 12(d).

Stage II is about information sharing systems and application of the privacy policy. The ISE Privacy Guidelines implement the requirements of IRTPA and EO 13388, which states that agencies protect information privacy rights and provide other legal protections relating to civil liberties and the legal rights of Americans; therefore, agencies will need to demonstrate their implementation and compliance with the ISE Privacy Guidelines. To assist agencies in identifying

[12] *An Introduction to the ISE Privacy Guidelines*, page 2.

which information systems and sharing arrangements involving protected information are part of the ISE, the same three steps—identify, assess, and protect—can be applied to Stage II.

- Step 1 is to identify the terrorism information systems, sharing arrangements, and protected information that are currently being shared or could be shared in the ISE.
- Step 2 is to assess those identified systems to ensure that the "protected information" covered by the sharing arrangements is handled in a manner consistent with the protections afforded by the ISE Privacy Guidelines.
- Step 3 is to protect by establishing actions that the agency needs to take for "protected information" shared from those identified systems. This stage may need to be repeated as new or additional systems and sharing arrangements in the ISE are developed and identified.

As a result of this effort, agencies will have two products that demonstrate their compliance with the ISE Privacy Guidelines. First, agencies will have formulated, either by documenting existing policies that satisfy the ISE Privacy Guidelines provisions and/or developing new policies, a privacy protection policy that complies with the basic privacy protections of the ISE Privacy Guidelines. Second, agencies will need to be able to demonstrate through documentation that they have applied this privacy protection policy to their systems and sharing arrangements in the ISE.

For purposes of this Implementation Guide, as described in the *Privacy Guidelines Committee Guidance Paper Suggested Approach for Applying Information Sharing Environment Privacy Guidelines*, the term "system" means information systems, databases, and data sets, as appropriate. The term "protected information," as defined in the ISE Privacy Guidelines, Section 1(b), means information about United States 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. 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. government expressly determines by Executive Order, international agreement, or other similar instrument should be covered by these Guidelines.

# Implementation Guide Format

This Implementation Guide recognizes that agencies employ various levels of privacy and civil liberties protections. Some agencies are required by law, Executive Order, policy, or procedure to undertake a variety of privacy information assessments and reviews. Other agencies may already have units or working groups that address privacy and civil liberties concerns related to their information sharing arrangements. It is not necessary to undertake new efforts or create new structures if existing ones will suffice to comply with the ISE Privacy Guidelines. Examples of existing activities, policies, and efforts that may satisfy a provision of the ISE Privacy Guidelines can be found in the Assistance Resources section. If an agency uses an existing activity or policy to satisfy an ISE Privacy Guidelines provision, the agency simply needs to document that use. Through this documentation, an agency can demonstrate its compliance with the ISE Privacy Guidelines.

The Implementation Guide is divided into three sections:

- Stage I
- Stage II
- Assistance Resources

Stages I and II describes for the user the required product associated with that stage, the authority for the required activities, and a discussion of the activity. This is meant to help agencies understand the scope of the activity and the various options or methods that could be used to address it.

The Assistance Resources Tab provides optional aids for an agency that desires assistance in addressing one of the steps. If an agency needs assistance in determining how to proceed through the steps identified in this document or would like additional background information on a topic, the Assistance Resources section can help. Throughout the document, the question mark symbol indicates where additional resources are available. The section contains optional aids, including checklists, model policies, best practices, and other tools, which are designed to assist an agency in addressing a particular activity. An agency is under no obligation to use the optional aids in the Assistance Resources section.

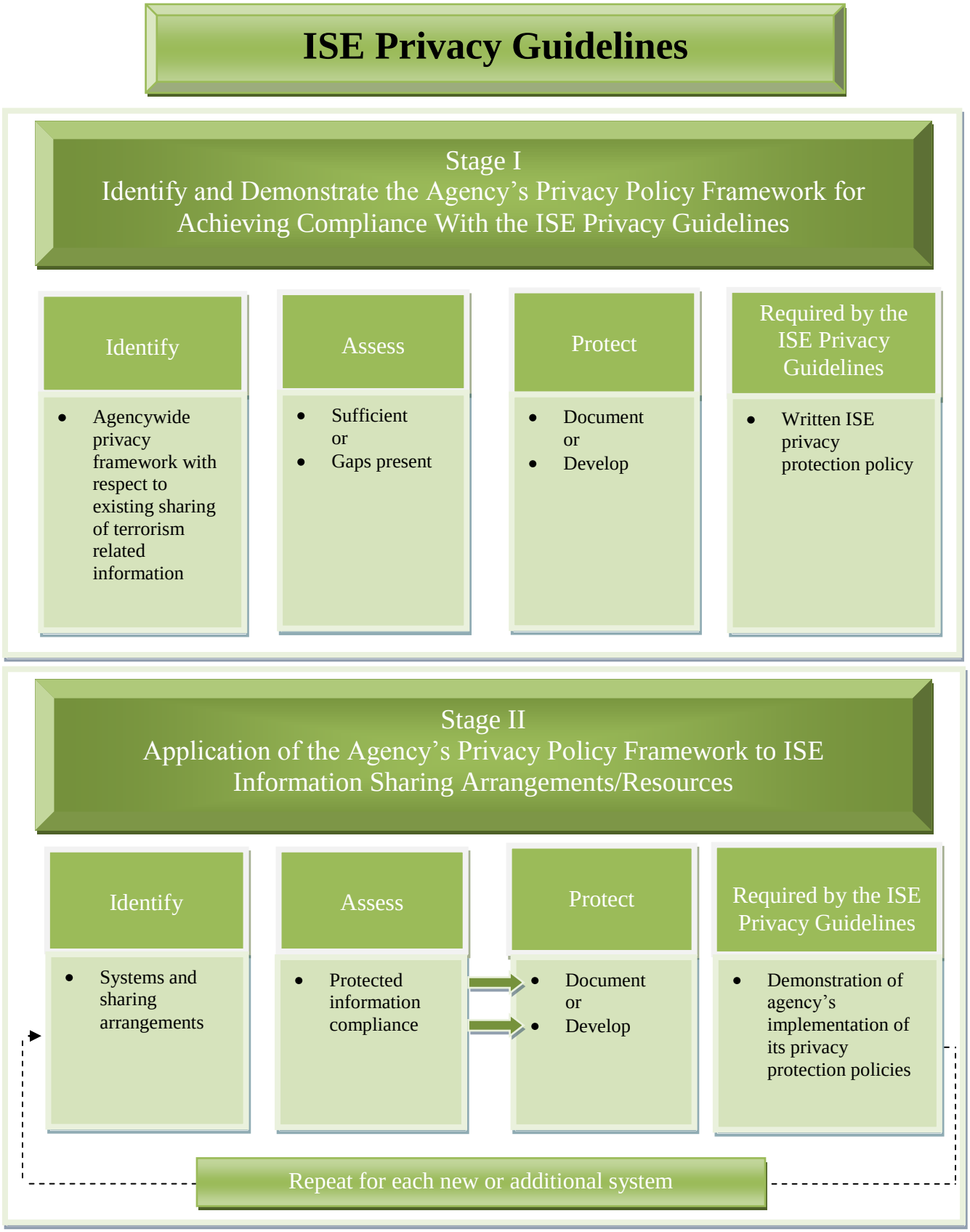


*Figure 1.1 Stages of Implementation*

# Stage I:
# Identify and Demonstrate the Agency's Privacy Policy Framework for Achieving Compliance With the ISE Privacy Guidelines

**Required Product:** Each Federal agency and department shall have a written ISE privacy protection policy (ISE Privacy Guidelines, Section 12(d)).[13]

**Discussion/Description:** To ensure that an agency has developed and implemented a written ISE privacy protection policy that complies with the ISE Privacy Guidelines, the agency will need to:

1) identify existing laws, Executive Orders, policies, and procedures that apply to protected information that will be available or accessed through the ISE (ISE Privacy Guidelines, Section 2 (a and b));
2) assess existing laws, Executive Orders, policies, and procedures that apply to protected information that will be available or accessed through the ISE to determine whether there are any gaps between existing protections and the protections identified in the ISE Privacy Guidelines (ISE Privacy Guidelines, Section 2 (b and c), Section 3, Section 5, Section 6, Section 7, and Section 8); and
3) protect privacy rights by documenting that existing laws, Executive Orders, policies, and procedures are in compliance with the ISE Privacy Guidelines **or** develop and adopt new policies that fill the gap(s) identified in 2), above (ISE Privacy Guidelines, Section 2 (c), Section 3, Section 5, Section 6, Section 7, and Section 8).

[13] *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*, December 2006, Governance, page 7.

# Stage I/Step 1:

**Identify—**Compile existing laws, Executive Orders, policies, and procedures that apply to protected information to be available or accessed through the Information Sharing Environment.

## Discussion/Description:

Determine and document the existing laws, Executive Orders, policies, and procedures that apply to protected information that is or will be made available or accessed through the ISE. Consider including terrorism information sharing practices that may be more informal as well as any proposed terrorism information sharing plans. The following list may provide an agency with a way to think about the scope of the laws, Executive Orders, policies, and procedures that need to be identified:

(a) Collection (acquisition and access)
(b) Retention (storage, safeguarding and validation)
(c) Production (dissemination and publication)
(d) Use (action and response taken upon receipt of such information)
(e) Sharing (dissemination of terrorism related information among ISE participants)
(f) Management (oversight and governance of the above practices and processes)

An agency's compilation of existing laws, Executive Orders, policies, and procedures should identify those authorities that apply to protected information available or accessed through the Information Sharing Environment.

Should you need assistance implementing Stage I/Step 1, consider using the additional resources provided in the Assistance Resources Tab.

# Stage I/Step 2:

**Assess—**Assess and identify gaps between existing protections and the protections identified in the ISE Privacy Guidelines.

## Discussion/Description:

**Assess "As-Is" State**—In considering whether its existing privacy and civil liberties protections are in compliance with those in the ISE Privacy Guidelines, an agency should assess what it is currently required to do. If an agency has already completed such a task, there is no need to repeat it. If not, then it may be useful to start with determining and documenting agencywide information privacy and civil liberties policies, procedures, guidelines, and practices.

Agencies may want to work with affected agency components to determine and document the agency's privacy and civil liberties legal and policy environment for terrorism information sharing. The issues to be reviewed might include:

(a) What legal authorities are controlling or relevant?
(b) What information may or may not be collected?
(c) How can information be collected?
(d) Who is eligible to receive information that is collected (both internally and externally)?
(e) What are the agency's transparency policies?
(f) What are the agency's redress policies?
(g) What are the agency's accountability, enforcement, and training policies?

Again, working with agency components, determine agencywide information privacy and civil liberties policies, procedures, guidelines, and practices. Consider reviewing the following items:

(a) Are the Fair Information Principles employed?
    — Privacy Act (PA) versus non-PA records?
    — Minimum necessary shared?
    — Limitations on redisclosure?
    — Alerts as to reliability?
    — Monitored disclosure?
    — Retention practices?
    — Security controls?
(b) Is commercial data (information obtained from a commercial source) collected or stored? How is it used? Are the following protections applied?
    — Sharing arrangements?
    — Reliability assurances?
    — Sharing alerts?
    — Verification requirements?

The result of an agency's assessment of the "as-is" state will be an understanding of which current laws, Executive Orders, policies, and procedures apply to the agency to allow comparison with the provisions in the ISE Privacy Guidelines. An agency may find it useful to identify or create a policy manual or other comprehensive repository of all privacy and civil liberties policies and procedures necessary for documenting consistency with the ISE Privacy Guidelines.

**Compare With the "To-Be" State and Identify Gaps**—Using the information gathered in the assessment of the "As-Is" state, an agency will need to compare what it is currently doing with what is required by the ISE Privacy Guidelines—the "To-Be" state. This comparison will help agencies determine whether their existing privacy and civil liberties protection policies adequately address those in the ISE Privacy Guidelines or whether there are gaps.

Based on the analysis of the legal and policy environment—including agency policies, procedures, and practices—an agency will need to identify areas where:

(a) No privacy and civil liberties policy or procedure exists.
(b) Required privacy policies and procedures are not adhered to.
(c) Privacy and civil liberties policies and procedures are misunderstood or lack implementing guidance.
(d) Existing privacy and civil liberties policy, procedures, or practices are insufficient to address the ISE Privacy Guidelines requirements.
(e) Training regarding privacy and civil liberties policies and procedures is inadequate or nonexistent and does not sufficiently address the ISE Privacy Guidelines requirements.

An agency may also want to consider the following questions:

(a) Does the agency seek and retain only what it is permitted to seek or retain?
(b) Is data only lawfully collected data?

In addition, an agency may want to take these steps:

(a) Identify interagency rules that impede sharing without protecting privacy and identify what purpose each restriction is designed to serve. If identified, raise issue with the Privacy Guidelines Committee.[14]
(b) Ensure that information identified as within the ISE, when shared via ISE processes, is used, consistent with the provisions of Executive Order 13388, for the detection, prevention, disruption, preemption, and mitigation of the effects of terrorist activities against the territory, people, and interests of the United States.

This agency's comparison will allow the agency to determine whether its existing privacy protection policies adequately address the ISE Privacy Guidelines. An agency may determine that its existing privacy and civil liberties protection policies satisfy ISE Privacy Guidelines requirements. Or an agency may determine that there are gaps in its privacy and civil liberties protection policies and that new policies need to be developed for the agency to be in compliance with the ISE Privacy Guidelines.

Should you need assistance implementing Stage I/Step 2, consider using the additional resources provided in the Assistance Resources Tab.

[14] ISE Privacy Guidelines, Section 12(b).

# Stage I/Step 3:

**Protect—**Develop an agency ISE privacy protection policy based on existing or developed legal and policy framework that fills all identified gaps and meets all the ISE Privacy Guidelines requirements, or document compliance of your existing systems.

## Discussion/Description:

Following comparison of an agency's existing privacy and civil liberties protection policies with the privacy and civil liberties protections in the ISE Privacy Guidelines, the agency will need to develop a written ISE privacy protection policy. An agency may document that its existing protections comply with the ISE Privacy Guidelines or develop new policies to fill the gaps. If an agency needs to develop new privacy and civil liberties protection policies, it may want to consider working with agency officials responsible for the ISE.

Documentation of existing policies or development of a new policy should address the following:

(a) A privacy protection policy stating that protected information shall be shared among agencies, organizations, and other persons only as allowed by the agency's information sharing policy and guidelines collected in a manual or held in a central repository.

(b) Protocols and guidelines for information sharing that:
- Define categories of information that may be shared.
- Define categories of entities with which data may be shared, with restrictions for each (e.g., law enforcement agencies, intelligence agencies, commercial entities, and individuals who are the subjects of records).
- Determine information sharing sources (e.g., systems of records/databases).
- Determine information sharing methods (e.g., software applications or other media).
- Determine how sharing requests may be received.
- Determine what processing must be conducted prior to sharing (e.g., formatting, redaction, and review).
- Determine information sharing protocols (encryption, de-identification/anonymization, documentation, and auditing).

(c) Memoranda of understanding, including terms and requirements regarding:
- Identity and authorities of information requester/receiver and sender.
- Required privacy and civil liberties protections (encryption, limited use agreements, data retention, notice and consent of data subjects where applicable, minimum necessary data shared).
- Required security protections (e.g., firewalls, intrusion detection systems, physical security, training and awareness of staff, and authorization and authentication).
- Dispute-resolution process.
- Rights in data, if applicable.
- Limitations on redisclosure.
- Effects of laws and regulations (including exemptions there from).
- Disclaimers of warranties/assurances of accuracy.
- Monitoring/auditing responsibilities of sender and receiver (e.g., methods, frequency, roles and responsibilities, and remediation).

In addition, documentation of existing policies or development of a new policy should address the following:

(a) An overarching policy for the periodic and careful review of agency and personnel compliance with privacy and civil liberties procedures (such as through an inspection/review process).
(b) An overarching mechanism for promptly reporting noncompliance with all ISE privacy and civil liberties procedures.
(c) An overarching mechanism for responding to incidents of noncompliance, including sanctions for individuals who are negligently or willfully noncompliant.
(d) Policies on computer matching and other data merges, including implications of the Privacy Act.
(e) Posting of Systems of Record Notices (SORNs) and other Privacy Act requirements, if applicable.
(f) Data accuracy, completeness, and timeliness controls.

For agencies developing new policies to fill identified gaps, the new policy and/or procedure should address the following:

(a) The relevant Federal laws, regulations, guidelines, interagency agreements or rules, or other agency-specific directives driving each requirement, especially those restricting data sharing.[15]
(b) The specific mandatory required action or end state.
(c) Any exemptions to each requirement that the agency may invoke or has invoked, if applicable.
(d) The specific officials and personnel affected and those responsible for implementation and oversight.
(e) The particular detailed procedures to be followed by each category of affected staff, including enforcement and assurance responsibilities.

The result of an agency's documentation that existing privacy protection policies comply with the ISE Privacy Guidelines or the development of new policies is the production of the required product in ISE Privacy Guidelines, Section 12(d)—a written ISE privacy protection policy.

Stage I is now complete. Stage II will document an agency's application of the written ISE privacy protection policy to its systems and sharing arrangements in the ISE.

Should you need assistance implementing Stage I/Step 3: consider using the additional resources provided in the Assistance Resources Tab.

[15] Broad policy goals are made pursuant to existing requirements, i.e., all policies incorporated into the repository will be authorized by existing statutes, regulations, or guidelines. Nothing in this methodology should be construed to grant the ISE officer or other agency staff authority to create and enforce requirements not embodied by existing law.

# Stage II:
# Application of Agency's Privacy Policy Framework to ISE Information Sharing Arrangements

**Required Product:** Demonstrate implementation and compliance with the ISE Privacy Guidelines.

## Discussion/Description:

Once an agency has identified, assessed, and protected through development of an ISE privacy and civil liberties protection policy in response to the ISE Privacy Guidelines, the agency will need to:

1) Identify existing and planned systems, sharing arrangements, and protected information covered by the ISE Privacy Guidelines (ISE Privacy Guidelines, Section 4 (a and b));
2) Assess identified systems to ensure that the protected information covered by the sharing arrangements is handled in a manner consistent with the protections afforded by the ISE Privacy Guidelines (ISE Privacy Guidelines, Section 4(b)); and
3) Protect those systems/information shared in the ISE by establishing agency actions that demonstrate its compliance (ISE Privacy Guidelines, Section 7 and Section 9).

This stage may need to be repeated as each new or additional system with terrorism information and sharing arrangements that are in the ISE is developed and identified.

# Stage II/Step 1:

**Identify—**Identify existing and planned systems, sharing arrangements, and protected information covered by the ISE.

## Discussion/Description:

**Identify Systems and Sharing Arrangements and Protected Information—**Agencies will need to identify existing systems and databases that contain terrorism related information that will potentially be shared through the ISE. If agencies already have a process that covers this step, they do not need to do additional assessments of those systems solely for the purpose of the ISE Privacy Guidelines.

If, however, an agency has not undertaken such a process, it may want to consider using the following process:

(a) Systems of Records/Databases Identified as Category I (refer to the Implementation Manual, Tab II, Subtab A) and in the Green Pages.
   - Analyze the Green Pages to ensure that systems of records/databases are appropriately identified as Category I.
   - Identify any information sharing agreements and other arrangements that exist or are planned for these systems and databases.

(b) Systems of Records/Databases Identified as Category I and NOT in the Green Pages
   - Identify the agency's systems of records/databases that are clearly Category I, although not identified in the Green Pages.
   - Identify any information sharing agreements and other arrangements that exist or are planned for these systems and databases.

(c) Systems of Records/Databases Identified as Category II (refer to the Implementation Manual, Tab II, Subtab A).
   - Identify the agency's Category II systems of records/databases that contain a mix of terrorism and non-terrorism information.
   - Identify any information sharing agreements and other arrangements that exist or are planned for these systems and databases.

(d) Systems of Records/Databases Identified as Category III (refer to the Implementation Manual, Tab II, Subtab A).
   - Identify the agency's Category III systems of records/databases that contain information that is clearly not terrorism information but that may become subject to ISE sharing as part of a terrorism investigation.
   - Identify any information sharing agreements and other arrangements that exist or are planned for these systems and databases.

For systems of records/databases identified as Category II and III, identify the risk environment around systems of records/databases that contain personally identifiable terrorism information to determine whether special protections are warranted.

Questions to ask may include:

(a) Does the system of record/database contain sensitive information that is subject to privacy and civil liberties protections (e.g., personally identifiable information that reveals medical, financial, or religious information)?

(b) What specific protections must each category of information receive under legal, regulatory, or contractual obligations?
(c) What information privacy policies and practices are applied?
(d) Do privacy protection exemptions assigned to the data or system apply if the information is shared within the ISE?
(e) What is the likelihood that the data will be shared within the ISE?
(f) How could each category of information under consideration be exploited if it were inappropriately disclosed, accessed, or intercepted?
(g) What harms would result to an individual?
(h) What is the magnitude of the harms that would result—to an individual, an organization, or larger interests, such as those of the United States?
(i) What types of persons would be interested in inappropriately accessing, transmitting, or receiving each type of information, both inside and outside the agency maintaining it?

The result of an agency's identification of the systems and sharing arrangements that contain protected information will provide an agency with the universe of the systems and sharing arrangements that fall under the ISE privacy protection policy.

Should you need assistance implementing Stage II/Step 1, consider using the additional resources provided in the Assistance Resources Tab.

# Stage II/Step 2:

**Assess—**Assess identified systems to ensure that the protected information is covered by the ISE privacy protection policy.

## Discussion/Description:

**Assessment and identification of risks to privacy and civil liberties for terrorism databases (risk environment)—**Agencies will need to assess and identify the risk to privacy and civil liberties for the terrorism systems identified in Step 1.

Questions should include:

(a) Were the agency's risk assessment criteria applied to determine whether ISE information shared in the ISE should continue to be shared and, if so, whether special protections are warranted?

(b) Were the agency's risk assessment criteria applied to determine whether ISE information under consideration for sharing in the ISE should be shared in the ISE and, if so, whether special protections are warranted?

Assessment of agency implementation of laws and policies—Agencies will need to assess their implementation of laws and policies to those identified systems.

Questions should include:

(a) Is the agency's information privacy and civil liberties marking system that ensures information is handled in accordance with applicable legal requirements applied to ISE information? (Refer to Implementation Manual, Tab VI, Subtab B.)

(b) Are the agency's data quality procedures designed to ensure accuracy, timely correction, and appropriate retention of data applied to ISE information? (Refer to Implementation Manual, Tab VI, Subtab C.)

(c) Are the agency's data security procedures designed to safeguard protected information applied to ISE information? (Refer to Implementation Manual, Tab VI, Subtab D.)

(d) Are the agency's auditing procedures designed to hold personnel accountable, ensure training of staff, and conduct reviews and audits designed to obtain and verify compliance applied to ISE information? (Refer to Implementation Manual, Tab VI, Subtab E.)

(e) Are the agency's transparency and redress procedures designed to inform the public of agency information and privacy policies and to address complaints from persons regarding information under agency control in place for the ISE? (Refer to Implementation Manual, Tab VI, Subtab A.)

The result of an agency's assessment and identification of risks to privacy in databases containing terrorism information and its assessment of whether laws, Executive Orders, policies, and procedures protecting privacy are implemented consistent with the ISE Privacy Guidelines will demonstrate an agency's application of the privacy and civil liberties protection policies.

Should you need assistance implementing Stage II/Step 2, consider using the additional resources provided in the Assistance Resources Tab.

# Stage II/Step 3:

**Protect—** Protect systems and information shared in the ISE by documenting an agency's actions, such as training, reporting, and audits.

## Discussion/ Description:

An agency will need to document the protections it employs to demonstrate implementation and compliance with the ISE Privacy Guidelines. The agency may not need to implement any new activities. If existing policies or procedures address the required provision, the agency simply needs to document that an existing policy or procedure complies with the ISE Privacy Guideline provision.

An agency should consider the following:

a) Put in place a policy that implements required protections for the system.
b) Put in place reporting/notification procedures regarding violations of agency-protection policies, as appropriate, that address reporting, investigating, and responding to such violations.
c) Put in place audit and enforcement mechanisms for the system as required by policy for that system.
d) Provide training for personnel authorized to share protected information for the system regarding the agency's requirements and policies for collection, use, and disclosure of protected information, and as appropriate for reporting violations of agency privacy and civil liberties protection policies.
e) Ensure cooperation with audits and reviews by officials with responsibility for providing oversight with respect to the ISE.
f) Ensure that the agency's designated ISE privacy official receives reports (or copies) regarding alleged errors in protected information that originates from the agency.

The result of an agency's documentation of its protections required for specific systems/information shared in the ISE, based on assessment of systems and policy requirements, will demonstrate its implementation and compliance with the ISE Privacy Guidelines.

Should you need assistance implementing Stage II/Step 3, consider using the additional resources provided in the Assistance Resources Tab.