



ENTERPRISE PRIVACY OFFICE



February 2016
version 1.0



 **admin**
THE SOUTH CAROLINA
DEPARTMENT *of* ADMINISTRATION



Document Purpose

The purpose of this document is to guide State of South Carolina agency staff through the process of conducting and documenting a Privacy Threshold Analysis and Privacy Impact Assessment.

Questions regarding this guide may be directed to the respective Agency Privacy Liaison.

Document Revision History

Table 1 - Document Revision History

Date	Authored by	Title	Ver.	Notes
12/16/2016	EPO		1.0	

Table of Contents

Guidance

I. Introduction.....	1
II. Scope	1
III. Process	2
a. Preparation.....	2
b. Privacy Threshold Analysis (PTA).....	2
c. Privacy Impact Assessment (PIA).....	3
d. Mitigation Plan	5
e. Frequency	5
IV. Tips for PTA/PIA Implementation	5
a. Writing Tips.....	5
b. Roles and Responsibilities.....	5

Appendices

Appendix A: Instructions for Completing PTA/PIA	A-1
Privacy Threshold Analysis (PTA)	A-2
Section 1.0: General Information	A-2
Section 2.0: Overview.....	A-3
Section 3.0: Data Characteristics.....	A-3
Privacy Impact Assessment (PIA).....	A-4
Supporting Documentation	A-4
Section 1.0: Data Collection.....	A-4
Section 2.0: Data Use	A-5
Section 3.0: Data Retention.....	A-5
Section 4.0: Data Sharing	A-6
Section 5.0: Notice to Individuals to Decline/Consent Use.....	A-6
Section 6.0: Individual Requests for Access, Redress, and/or Correction	A-6
Section 7.0: Access Privileges and Security	A-7
PTA/PIA Findings and Mitigation Plan	A-8
Appendix B: PTA/PIA Template	B-1
Appendix C: Findings and Mitigation Plan	C-1

Executive Summary

Each Agency is required by SCDIS-200 Information Security and Privacy Standard Control 12.400, Data Protection and Privacy to ensure that the interests of data subjects are appropriately protected, The *Agency Guidance and Template for Completion of the Privacy Threshold Analysis/Privacy Impact Assessment (PTA/PIA)* is designed to assist Agencies in meeting this requirement.

Section I introduces the framework and methodology involved in PTA/PIAs.

Section II discusses the scope of the PTA/PIA and how data classification supports this assessment.

Section III describes the process of conducting the PTA/PIA, defines important privacy concepts and terminology, and maps how often Agencies should conduct PTA/PIAs.

Section IV recommends tips to help streamline the PTA/PIA process, including defining the individual roles and responsibilities.

Appendix A contains instructions for completing the PTA/PIA.

Appendix B is the PTA/PIA template.

Appendix C is a template for documenting the mitigation plan addressing risks identified by the PTA/PIA.

Agency Guidance for Completion of the Privacy Threshold Analysis and Privacy Impact Assessment

I. Introduction

The State of South Carolina Government has the ongoing responsibility to balance individuals' privacy rights with the State's mandate to provide services. Each Agency is required by SCDIS-200 Information Security and Privacy Standard Control 12.400, Data Protection and Privacy, to ensure that the interests of data subjects are appropriately protected. The completion of a Privacy Threshold Analysis/Privacy Impact Assessment (PTA/PIA) demonstrates compliance with this standard. This guidance provides a framework for conducting a PTA/PIA.

II. Scope

Each Agency accomplishes its **mission** by establishing multiple business processes. The **business processes** involve information technology systems and manual processes. Groups of information, or **data sets**, are required for the business processes to be executed. The data sets are comprised of individual **data elements** collected, used, shared, retained, and disposed of, over the course of the business process.

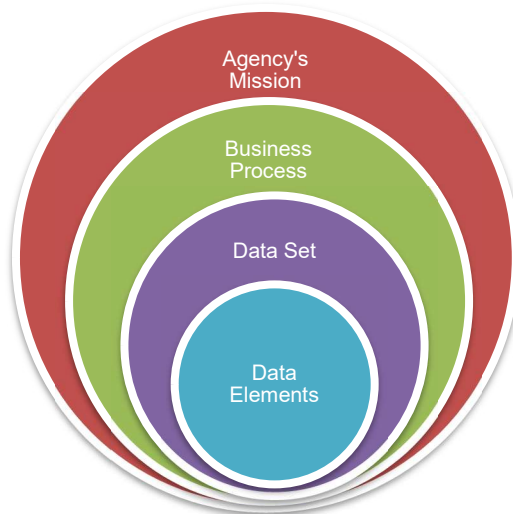


Figure 1: Relationship Data Elements to Agency Mission

Data elements exist in electronic, as well as, paper-based format, and may include Personally Identifiable Information (PII). In general, PII is information that, whether alone or when combined with other information, is linked or linkable to a specific individual. ('Linked' and 'linkable' refer to the ability to make a logical association between different sets of information.)

Table 1: Examples of PII

Stand-Alone Data Elements		
Social Security Numbers	Personal Email Address	Personal Bank Account Numbers
Name	Credit Card Number	Driver's License Number
Tax Identification Number of a Sole Proprietor	Passport Number	State Identification Card Number
Data Elements that, when Combined, may be Linked, or Linkable, to One of the Above		
Place of Birth	Race	Religion
Medical Information	Education Information	Financial Information
Geographical Indicators, e.g. zip code	Employment Information	Date of Birth

Special protections are placed around PII because the unauthorized use of, or access to, PII may cause harm to the individual. Harm includes such things as financial fraud, medical identity theft, and embarrassment.

The PTA/PIA process assesses whether an Agency's business process contains PII, and then analyzes how that business process collects, uses, shares, retains, and disposes of the PII.

III. Process

a. Preparation

In preparation for the conduct of Agency PTA/PIAs, it is *highly* recommended that the Agency first complete its data classification. During data classification the Agency documents its major business processes (System Level Tab of the Data Inventory Tool Spreadsheet), the data elements collected for executing those business processes, and the data classification category. Having this information documented prior to the PTA/PIA process will significantly streamline the timeline.

For information on the State of South Carolina Data Classification Schema and the Data inventory Tool Spreadsheet, go to <http://www.admin.sc.gov/technology/enterprise-privacy/policy-and-guidance>.

b. Privacy Threshold Analysis (PTA)

The purpose of the PTA is to document that a review has been conducted to determine whether a business process involves the collection, use, sharing, retention, or disposal of PII. The determination of whether or not PII is involved in the business process should be documented in the Privacy Threshold Analysis/Privacy Impact Assessment Findings and Mitigation Plan (Appendix C).

If PII is not identified, no further privacy risk analysis is warranted.

If PII is identified, a Privacy Impact Assessment (PIA) is required.

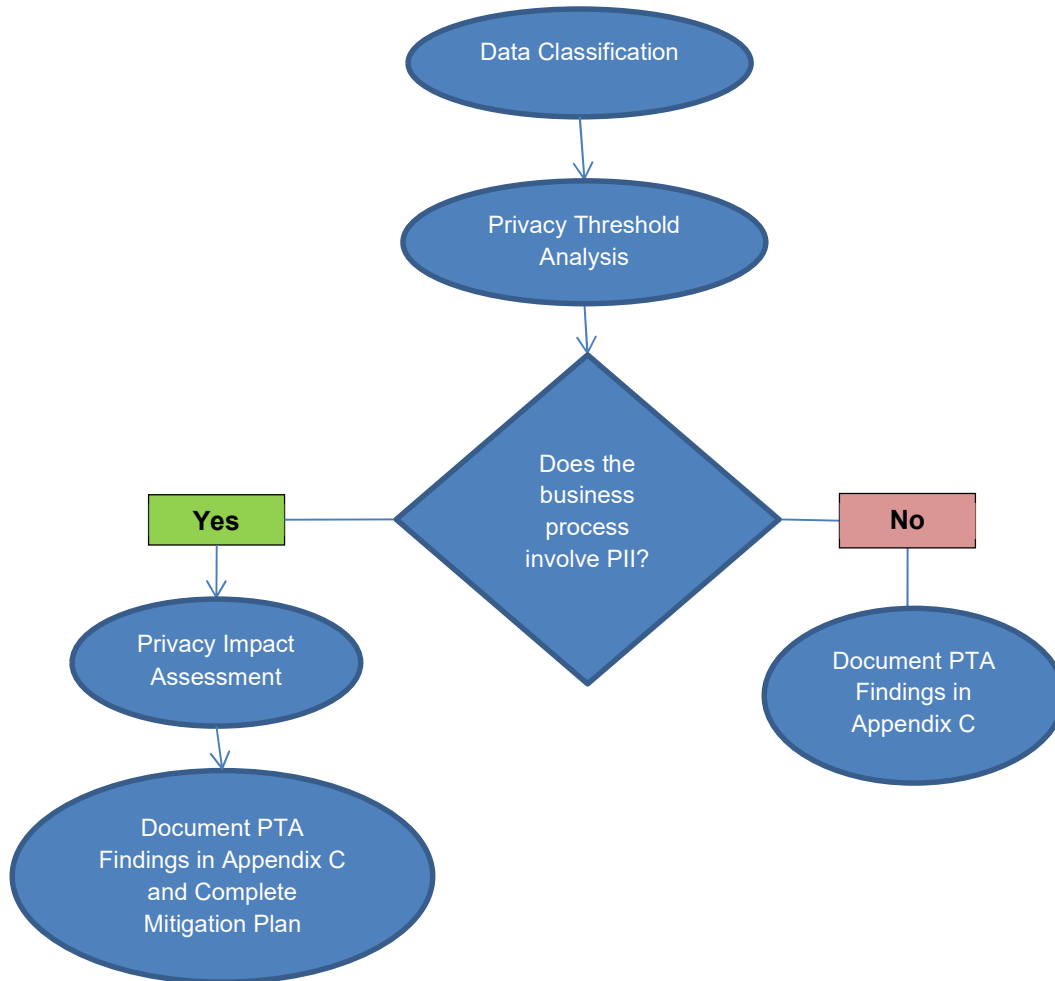


Figure 2 - PTA/PIA Process

c. Privacy Impact Assessment (PIA)

A PIA is an analysis of how PII is handled during a specific business process. The purpose of the PIA is to:¹

- Ensure information handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;
- Determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form; and

¹ U.S. Office of Management and Budget Memorandum, M-03-22, "Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002"

- Examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

The State of South Carolina PIA prompts an Agency to assess its data collection, use, disclosure, and retention practices against widely accepted principles used in the evaluation and consideration of systems, processes, or programs affecting individual privacy. The following underlying privacy principles² form the basis for a comprehensive assessment of the Agency's business processes and are the framework for the questions contained in the PTA/PIA template.

- **Notice and Transparency:** Inform the individual about what personal information is being collected and how that information will be used and shared. This is sometimes referred to as "providing notice." Communications should be in plain language and accessible to the individual.
- **Use and Disclosure Limitation:** Use and disclose an individual's information only in the manner described in the notice. Uses and disclosures outside of the notice require explicit consent from the individual, except for certain instances, such as law enforcement requests.
- **Individual Participation, Access, and Redress:** Provide individuals with a reasonable opportunity to consent to the collection, use, or disclosure of personal information. Provide individuals with procedures on how to access information being held about them, how to correct or update that information, and whom to contact with further questions.
- **Data Minimization and Retention:** Collect only the information needed to perform the official business of the State of South Carolina. Retain information collected for a specific business purpose only as long as necessary to fulfill the purpose for which it was collected, or as required by Agency records retention and/or other policies and/or other State or federal laws and/or regulations.
- **Data Quality and Integrity:** Establish policies and procedures to ensure, to the greatest extent practicable, that data is accurate, complete, and up-to-date.
- **Security:** Establish the appropriate management and operational administrative, technical, and physical safeguards to preserve the privacy, confidentiality, integrity, and accessibility of personal information. These safeguards should align with the level of protection afforded to data categories assigned, using the State of South Carolina Data Classification Schema.

² The privacy principles are drawn from several widely accepted frameworks of defining principles used in the evaluation and consideration of systems, processes or programs affecting individual privacy, including:

- Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)
<http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm>
- Privacy Act of 1974, 5 U.S.C. § 552a, as amended <http://www.justice.gov/opcl/overview-privacy-act-1974-2015-edition>
- U.S. Department of Health, Education and Welfare report, "Records, Computers and the Rights of Citizens" (1973) <http://www.justice.gov/sites/default/files/opcl/docs/rec-com-rights.pdf>

- **Accountability and Auditing:** Establish policies and procedures assigning information protection roles and responsibilities, and institute processes for evaluating compliance, effectiveness, and improvement.

d. Mitigation Plan

Privacy risks identified by the PIA should be documented in a mitigation plan (Appendix C). The plan should describe the risk to be addressed, the action plan to mitigate the risk, who will be responsible for completing the action and the timeline for completion.

e. Frequency

An Agency should conduct a PTA/PIA:

- Prior to implementing new business processes, *and*
- When changes are made to existing business processes which may impact data collection, use, retention, or sharing, or introduce new privacy risks, *or*
- At least every three years on each business process.

IV. Tips for PTA/PIA Implementation

a. Writing Tips

Below are some helpful hints for writing the PTA/PIA documents:

- Use plain English.
- Be brief in your response, but detailed enough to convey the specifics of the data and business process.
- Answer all questions completely.
- Explain acronyms upon first use.
- Define technical terms or references.
- Cite relevant legal references or previously published documents, where appropriate.

b. Roles and Responsibilities

The following roles and responsibilities are recommended for PTA/PIA completion.

System Owner – Designated by the Agency to control access to the Agency’s data records that are the subject of the PIA (i.e., the person setting the criteria for data access level determinations); usually the program manager for the business process. Responsible for overall coordination and completion of the new or updated PTA/PIA, but may assign a primacy point of contact to compile, review, and update the PTA/PIA. The System Owner may rely on the advice of the Security Reviewer and/or other security staff. The System Owner is responsible for submitting the completed PTA/PIA to the Privacy Liaison.

Primary Point of Contact– Designated by the System Owner to compile, review, and/or document the PTA/PIA. May work with the Privacy Liaison, Security Reviewer, and other staff to gather all necessary information needed to complete the PTA/PIA.

Security Reviewer – Authorized by the Agency to determine whether or not risks associated with information security can be accepted (See SC DIS Control 4.205).

Privacy Liaison – Designated by the Agency as the liaison between the Agency and the Enterprise Privacy Office (EPO). Verifies the accuracy of PTAs that indicate no PII is involved in the business process. Analyzes PIAs, and, in conjunction with the System Owner, develops an action plan to mitigate privacy risks identified by the PIA.

Appendix A
Instructions for Completing PTA/PIA Templates

This section provides an explanation of each question in the PTA/PIA template. Section headings are hyperlinked to the correlating section of the PTA/PIA template to allow for easy transition between the instructions and template question.

Privacy Threshold Analysis (PTA)

Section 1.0 General Information

Business Process- Identify the specific business process for the Agency. Consider using the Agency's completed Data Classification spreadsheet to ensure continuity.

Agency Name- Provide the Agency Name <http://sc.gov/Pages/agencyListingA-Z.aspx>. Please include the specific office or division.

PTA/PIA #- The PTA/PIA number will be assigned by the Agency liaison. The PTA/PIA tracking number will be used to maintain consistency and to track PTA/PIA documents throughout the privacy review process. An example of a naming convention follows.

Year- Current Year of submission to the Agency Privacy Liaison

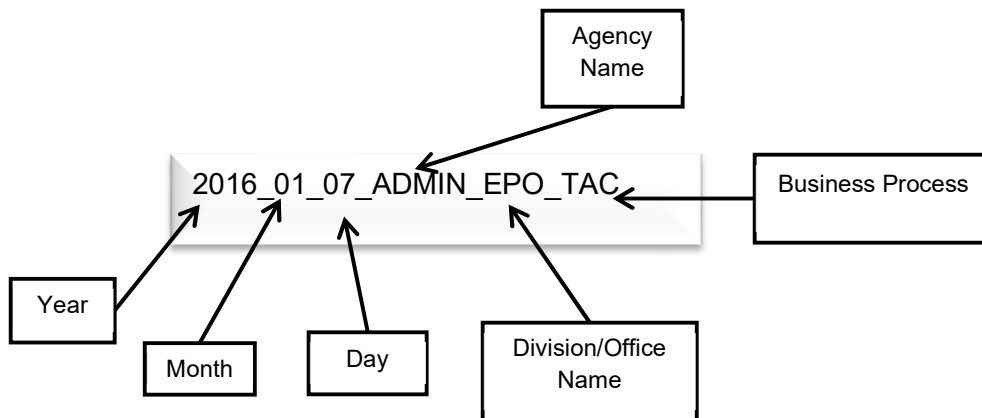
Month- Current Month of submission to the Agency Privacy Liaison

Day- Current day of submission to the Agency Privacy Liaison

Agency Name- Identify the specific Agency abbreviation

Division/Office Name- Identify the specific Division/Office responsible for the business process.

Business Process- The abbreviation of the business process will be used; use the first letter of each word in the business process. [For example Time and Compliance (TAC) or School Lunch Account Management (SLAM)]



System Owner- Insert the name/title of the system owner. The system owner should be the same person identified in the Data Classification spreadsheet.

Agency Privacy Liaison- Insert the name of the Agency privacy liaison.

New PTA/PIA?- If this is a new PTA/PIA, check yes. If this is an update to an existing document, check no. If no, provide the PTA/PIA number previously assigned by the Agency privacy liaison, and provide a brief description of the update or changes to the business process and correlating update to the PTA/PIA.

Section 2.0 Overview

Question 2.1- Provide a description of the business process and how it supports the Agency's mission. Describe, in general terms, how the data set is collected, used, shared, retained, and/or disposed of, during the business process, including whether the data set is paper-based, electronic, or a hybrid. If applicable, identify the name of the application/system that is used to support this process.

Section 3.0 Data Characteristics

Question 3.1- Identify all PII the business collects, uses, retains, and/or shares. If the system collects something that is not specifically identified, please select "other" and identify the item(s).

Question 3.2- Identify the source of the information collected by the business. For example, is the information provided directly by the individual, either manually or transferred from another business or system, or is the information provided from a Federal, State, County, or Local agency?

Question 3.3- Identify how the Agency's business process collects the information.

This last section of the PTA is to be completed by the Agency Privacy Liaison. The Agency Privacy Liaison will review the PTA and determine if additional information is needed to complete the document or if a full PIA is needed, based on the information presented in the PTA.

Privacy Impact Assessment (PIA)

Supporting Documentation

Supporting documentation may be required by the Agency Privacy Liaison to help ensure a full understanding of the business process, data flow, and safeguards. Examples of documents that may be requested are business process data flow mapping, data collection tools, and data sharing agreements.

Section 1.0 Data Collection

Questions 1.1 and 1.2- These questions were asked in the PTA. The response should be copied to the PIA and include additional details to describe the source of the information, and how the information is collected.

For example: Individuals provide their name, social security number, date of birth, address, etc. when requesting a new identification card. The information is collected from the individual requesting the new identification card and is then entered into the XYZ Database for processing. Once information has been entered into the database, all paper documents are placed in a secure container for shredding.

For example: Agency J sends an encrypted, one way transmission of data once a week. The information that Agency J sends includes the individual's name, home address, and whether or not the individual is covered by health insurance. Please see submitted Memorandum of Understanding between XYZ Agency and Agency J.

Question 1.3- Describe why this business process collects, uses, shares and/or retains this PII and why the collection of this information is necessary to the program or Agency mission. Include the context and background necessary to understand the purpose of the business process. Also include any sub-processes, program office names, applications/systems, and/or technology that support the business process.

Question 1.4- Describe how the information collected is checked for accuracy. What are the steps the Agency takes to ensure the information is accurate, relevant, timely and complete. This may include verifying data as it is collected or entered into an application/system, verifying the sources of data if not collected directly from the individual, and ensuring individuals who submit their PII are allowed to revalidate the information. If individuals are required to revalidate information, how often are they required to revalidate?

Question 1.5- Identify the federal, State, and regulatory requirements that give the business the authority to collect the information from individuals. Provide the specific citation or regulation.

Question 1.6- Indicate if the business process is covered by any of the following regulatory compliance privacy requirements.

- Health Information Technology for Economic and Clinical Health Act (HITECH Act)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Criminal Justice Information Services (CJIS)
- Family Educational Rights and Privacy Act (FERPA)

- Payment Card Industry-Data Security Standard (PCI-DSS)
- Internal Revenue Service (IRS) Publication 1075

If the business process is covered by another regulatory compliance privacy requirement not identified above, please provide the citation and a brief description of compliance privacy requirement.

Section 2.0 Data Use

Question 2.1- List each use of the information collected or maintained. Provide a detailed description of how and why the different data elements will be used. Each data element identified in Section 3.0 (Data Characteristics) of the PTA should be addressed.

For example: The business collects name, address, phone number, date of birth, spouse information for the emergency contact database.

Section 3.0 Data Retention

Question 3.1- For each of the data elements identified in the PTA, indicate how the Agency retains the information. Describe the steps the Agency takes to ensure the information is secured.

For Example: Information can be retained in file cabinets, storage rooms, or an electronic database. Describe the steps the Agency takes to ensure this information is secure.

If an Agency has contracted with third parties to store files or for database management, ensure the third party adheres to the defined Agency retention policy.

Question 3.2- Contact the Agency Records Officer to determine the specific retention schedule. The Agency Records Officer will review the types of information used and identify the correct retention schedule and any exceptions or limitations based on the retention schedule. Include all applicable retention schedules that apply to the type of data that is collected in the business process.

Question 3.3- Provide a detailed explanation of the how the Agency disposes of PII once the PII is no longer relevant and necessary to the business process. The PII should be maintained in accordance with the Agency's approved retention schedule(s) and disposed of using the approved Agency method to ensure secure deletion or destruction of the PII, including shredding, erasing, and anonymizing the PII, in a manner that prevents loss, theft, misuse, or unauthorized access.

Question 3.4- Provide information on documentation of disposal procedures. Is compliance with these procedures audited, and if so, how often?

Question 3.5- Describe how the records are maintained and stored. If records are maintained and stored in an offsite facility, provide the name of the facility and the procedures currently place for storing PII. If there is an agreement between an agency and another entity to provide records storage and maintenance services, provide a brief description of the services.

Section 4.0 Data Sharing

Describe if the business process allows for sharing of data, either internal (to State of South Carolina governmental entities) or external (outside of the State of South Carolina governmental entities). In Sections 4.1 and 4.3, provide the name of the entity with whom data is being shared; the purpose of the data sharing; the specific data elements being shared (data elements were previously identified in question 3.1 of the PTA); method used to share the data; and what safeguards are currently in place to protect the data as it is being transmitted.

Section 5.0 Notice to Individuals to Decline/Consent Use

Question 5.1- Describe the method used to provide individuals with notification prior to the collection of information. This may include providing individuals with a privacy notice from the website or a letter or form prior to the individual providing information. If the individuals are not given notice prior to submitting their personal information, please explain why notice is not provided.

Question 5.2- Indicate whether individuals are allowed to decline to provide information; yes or no. If the answer is yes, answer Question 5.3; if the answer is no, answer Question 5.4.

Question 5.3- If individuals are allowed to decline to provide their information, what are the consequences or the impact of the individuals not providing their information.

For Example: If an individual declines to provide his/her personal information, the individual may not receive the necessary requested assistance. When an individual refuses to provide his/her personal information to the intake worker, the intake worker must relay this information to a manager. The manager is responsible for carefully explaining the consequences of not providing the necessary personal information during the intake process.

Question 5.4- If an individual is not allowed to decline to provide information, but does not receive notification prior to the collection, provide a detailed justification to explain why notice was not provided to the individual.

Question 5.5- Describe how individuals are informed of their rights to consent to particular uses of their information. Does the collection of information cover all uses (current or potential), or is the information provided for a specific purpose and consent must be given for each use? If consent is required for each use, how does an individual provide consent?

Section 6.0 Individual Requests for Access, Redress, and/or Correction

Question 6.1- Describe the procedures an individual can use to request access to his/her personal information and/or correct erroneous information the agency has collected. Methods of providing the individual with the procedures needed to request access, or correct erroneous information, can include posting the agency's address or contact information on any form or on the website.

For Example: Individuals requesting access to the information must submit a request, in writing, to view the information the agency has collected. The procedures for requesting access are documented on the intake form and given to the individual at the time the information is submitted.

Question 6.2- Describe how individuals are informed of their rights and the process through which to appeal a decision if the individual is dissatisfied with the agency's initial response to the request for access or correction. This could include providing an individual with information on the appeals process, either during the intake process or at the time a decision has been made.

Section 7.0 Access Privileges and Security

Question 7.1- Describe the policies or procedures used to assign roles and provide access to the system and data. How are changes made once a person has received access to a system? Include any supporting documents, such as technical and/or operational manuals or security plans.

Question 7.2- If contractors are involved in development, design, or maintenance of the business process/system, how are privacy-related safeguards addressed? Describe the privacy related safeguards and requirements built into the contract.

Question 7.3- Describe how individuals, who have access to the data, are made aware of the privacy safeguards in place for the business process.

Question 7.4- Has Information Security reviewed the business to determine if it is compliant with the SC DIS 200 Standard 1.400?

For Example: During the review of the business did Information Security identify any risk? If so, include a brief description of the identified risk and how the risks are being addressed and mitigated by the business process. Has the Agency Chief Information Security Officer or his/her designee reviewed the identified risks and documented the decision to accept the risk?

Question 7.5- Describe the physical, administrative, and technical controls currently in place to protect the information.

For Example: Information collected is stored in a locked file cabinet in a storage room, which requires key card access. Individuals requiring access to this information must request access from the Division Director (in writing).

PTA/PIA Findings and Mitigation Plan

The PTA/PIA Mitigation Plan is used to assess the privacy risk identified while completing the Privacy Impact Assessment (PIA).

If no PII is found in the business process, and it is not necessary to complete the PIA, answer the first question, “No.” No additional information is needed.

Risk #	Description of Privacy Risk	Planned Mitigation Action	Person Responsible for Mitigation Action	Projected Completion Date	Status	Comments
--------	-----------------------------	---------------------------	--	---------------------------	--------	----------

If PII has been identified in the business process, the mitigation plan should be completed.

Risk #- The risk number is used to track the privacy risk.

Description of Privacy Risk- Provide a brief description of the privacy risk identified after completing the PIA.

For Example: After entry of data into electronic database, hard copies of forms containing PII are filed in an ununlockable cabinet located in an open area.

Planned Mitigation Action- Describe what steps the business process will take to mitigate the risk.

For Example: Immediately move file cabinet into supervisor’s lockable office. Determine whether Agency policy and/or records management policy requires retention of completed forms, and if so, for how long. Dispose of forms in locked shred bin and/or transfer forms to lockable file cabinet, as appropriate. Update procedures.

Person Responsible for Mitigation Action- Identify the primary person who will be responsible for ensuring the mitigation is completed. This person could be the system owner.

For Example: Jane Supertech

Projected Completion Date: Provide the current status of the privacy risk; use IP (In Progress), C (Closed), and D (Delayed).

In Progress should be used once any activities to resolve the risk have begun. Such activities can include planning, procurement, coordination, and/or remediation activities.

Closed should be used only once the risk has been properly addressed and approved by the Privacy Liaison. When a risk is closed, provide details in the comments section to identify the actions taken.

Delayed should be used if actions for the risk will, or have gone, beyond the Projected Completion Date. When a risk is delayed, provide details in the comments section to identify the reason for delay.

Comments: Use this section to provide updates to the privacy risk or the actions taken to close the risk, or update in the case of a delay.

For Example: There is no requirement to retain completed forms in paper format after the data has been entered into the electronic database. Forms have been disposed of in a locked shed bin, procedures have been updated, and all Agency staff has been informed through an email sent on November 1, 2015, by the Agency's records officer.

Appendix B
PTA/PIA Template

Business Process: _____ PTA/PIA#: _____

Privacy Threshold Analysis (PTA)

The purpose of the Privacy Threshold Analysis is to document that a business process has been reviewed, for the purpose of determining whether or not the process involves Personally Identifiable Information (PII).

Section 1.0 General Information

Business Process:			
Agency Name		PIA/PTA #	<Enter PTA/PIA# # assigned by the Agency Privacy Liaison or if this is an update to existing PTA/PIA, enter the original PTA/PIA #>
System Owner			
Agency Privacy Liaison:			
New PTA/PIA?	<input type="checkbox"/> Yes <input type="checkbox"/> No, update to an existing PTA/PIA		
If this is an update to an existing PIA, include the initial PTA/PIA Number and a reason for the update:			

Section 2.0 Overview

<p>2.1 Provide a brief overview of the business purpose: <i>Briefly describe the data set, including:</i></p> <ul style="list-style-type: none"> <i>The business purpose of the Agency and how the Agency's data elements support the program and Agency mission;</i> <i>A general description of the information in the data set's data records,</i> <i>Whether the data elements are paper-based, electronic or a hybrid.</i>

Business Process: _____ PTA/PIA#: _____

Section 3.0 Data Characteristics

3.1 What Personally Identifiable Information (PII), contained in the Agency data set, is collected, used, retained, or shared? (Check all that apply.)			
<input type="checkbox"/> Social Security Number	<input type="checkbox"/> Name	<input type="checkbox"/> Spouse Information	<input type="checkbox"/> Personal Cell Phone
<input type="checkbox"/> Driver's License Number	<input type="checkbox"/> Date of Birth	<input type="checkbox"/> Security Clearance	<input type="checkbox"/> Office Phone Number
<input type="checkbox"/> Passport Number	<input type="checkbox"/> Place of Birth	<input type="checkbox"/> Law Enforcement	<input type="checkbox"/> Office Direct Phone Number
<input type="checkbox"/> Personal Credit or Debit Card Number	<input type="checkbox"/> Home Address	<input type="checkbox"/> Emergency Contact	<input type="checkbox"/> Work Email Address
<input type="checkbox"/> Personal Financial Information	<input type="checkbox"/> Maiden Name	<input type="checkbox"/> Military Status/Service	<input type="checkbox"/> Biometrics
<input type="checkbox"/> Taxpayer ID	<input type="checkbox"/> Gender	<input type="checkbox"/> Employment Information	<input type="checkbox"/> User ID
<input type="checkbox"/> Employee ID	<input type="checkbox"/> Age	<input type="checkbox"/> Education Information	<input type="checkbox"/> IP Address
<input type="checkbox"/> Health Insurance Beneficiary	<input type="checkbox"/> Race/Ethnicity	<input type="checkbox"/> Other Names Used	<input type="checkbox"/> MAC Address
<input type="checkbox"/> Vehicle License Plate	<input type="checkbox"/> Personal Email Address	<input type="checkbox"/> Salary	<input type="checkbox"/> Occupation
<input type="checkbox"/> State Identification	<input type="checkbox"/> Religion	<input type="checkbox"/> Work Address	
<input type="checkbox"/> Mother's Maiden Name	<input type="checkbox"/> Medical Information	<input type="checkbox"/> Job Title	
<input type="checkbox"/> Other:			

3.2 What is the source of the PII collected? (Check all that apply.)				
<input type="checkbox"/> Individual	<input type="checkbox"/> SC State Agency	<input type="checkbox"/> Federal Agency	<input type="checkbox"/> County Agency	<input type="checkbox"/> Local Agency
<input type="checkbox"/> Other				

3.3 How is the information collected for this business process? (Check all that apply.)				
<input type="checkbox"/> Paper Format	<input type="checkbox"/> In-Person Interview	<input type="checkbox"/> Facsimile	<input type="checkbox"/> Telephone Interview	<input type="checkbox"/> Email
<input type="checkbox"/> Website	<input type="checkbox"/> Interagency Sharing	<input type="checkbox"/> Other		

Business Process: _____ PTA/PIA#: _____



Please stop here, and submit this form to the Agency Privacy Liaison.

Agency Privacy Liaison:	
Does the business process/system contain PII?	Yes <input type="checkbox"/> (If Yes, complete the PIA) No <input type="checkbox"/>
Comments:	

Privacy Impact Assessment (PIA)

The purpose of the Privacy Impact Assessment is to analyze how Personally Identifiable Information (PII) is handled within the business process, and identify privacy risks.

Supporting Documentation

The Privacy Liaison will need access to the following supporting documentation. Please ensure these documents are available when submitting the PIA for review.

- **Data flow mapping of business process-** This mapping should provide a visual depiction of data movement throughout the business process, from collection to disposal.
- **Data collection tools-** This includes hard copy forms, webpages, surveys, and any other methods for collecting an individual’s data.
- **Data sharing agreements-** This includes memoranda of agreement/memoranda of understanding, contracts, and other documentation associated with sharing Agency data records within, or outside of, State government.

Section 1.0 Data Collection

1.1 What is the source of the PII collected for this business process? (Check all that apply.) <i>This information can be copied from the PTA.</i>				
<input type="checkbox"/> Individual	<input type="checkbox"/> SC State Agency	<input type="checkbox"/> Federal Agency	<input type="checkbox"/> County Agency	<input type="checkbox"/> Local Agency
<input type="checkbox"/> Other				
Describe:				

1.2 How is the information collected by the business process? (Check all that apply.) <i>This information may be copied from the PTA.</i>				
<input type="checkbox"/> Paper Form	<input type="checkbox"/> In-person Interview	<input type="checkbox"/> Facsimile	<input type="checkbox"/> Telephone Interview	<input type="checkbox"/> Email
<input type="checkbox"/> Website	<input type="checkbox"/> Interagency Sharing	<input type="checkbox"/> Other:		
Describe:				

1.3 What is the purpose for which the PII is being collected, used, shared, or retained? <i>Describe why the particular PII collected, used, shared, or retained in the business process is necessary to the program or Agency mission.</i>

1.4 How is the information checked for accuracy? <i>For example, is the information checked for accuracy through comparison with another source? Are individuals required to revalidate information?</i>

1.5 What is the legal authority for the collection of information? Provide the specific citations. <i>Examples may include federal statutes, State law, and/or regulations.</i>

1.6 What are the regulatory compliance privacy requirements?		
<input type="checkbox"/> HIPAA-HITECH	<input type="checkbox"/> GLBA	<input type="checkbox"/> CJIS
<input type="checkbox"/> IRS Publication 1075	<input type="checkbox"/> FERPA	<input type="checkbox"/> PCI-DSS
<input type="checkbox"/> Other (Provide the citation and a brief description)		

Section 2.0 Data Use

2.1 How is the information in the data sets used to support the Agency?

Section 3.0 Data Retention

3.1 What information is retained by the Agency? <i>This may include any third party organizations contracted to retain information for the Agency.</i>

3.2 How long is information retained, and under what retention schedule? <i>Describe any exceptions to the retention schedule. Consult your Agency Records Officer or Agency General Counsel for advice regarding information retention schedules.</i>

3.3 What are the Agency's procedures for the disposal of information at the end of the retention period?

Describe policies and procedures for how PII that is no longer relevant and necessary is purged. This information may be obtained from the Agency Records Officer or Agency General Counsel.

Example: Paper records are shredded, in accordance with DIS Information Security and Privacy Standards, by a vendor under contract with the State. The disposal is documented by way of a certificate of destruction.

3.4 Where are the procedures documented? How are disposal procedures audited for compliance?

3.5 Where is information maintained or stored?

Example: XYZ Agency currently has a contract with VendorStore USA, Inc. The data is stored on servers located in a secure facility in Charlotte, NC.

Example: XYZ Agency currently has an (ISA/MOU) with the Division of Technology (DT). The servers are located at the Broad River Road Facility.

Section 4.0 Data Sharing

4.1 Describe data sharing with State of South Carolina Government entities.				
<i>State of South Carolina Government Entity</i>	<i>Purpose for which information is shared</i>	<i>Specific information types that are shared</i>	<i>Method of transmittal or disclosure</i>	<i>Safeguards for data transmittal and disclosure</i>
<i>EX. MyFellow Entity</i>	Information is shared with MyFellow Entity A for mandatory reporting under law JKL.	Name, Work Address, Work Telephone Number, and Work Email Address	Weekly Secure File Transfer Protocol	Information shared with the MyFellow Entity is sent via a file transfer

4.2 What agreements, and other types of documentation, are in place, which establish parameters around the internal data sharing listed above, and how frequently are these documents reviewed?
<i>Examples: Memorandum of Agreement or Memorandum of Understanding (MOA/MOU) between Agency and Entity is reviewed annually. Contract XYZ is reviewed every three years.</i>

4.3 Describe data sharing with the non-State of South Carolina Government entities.				
<i>Non-State of South Carolina Government Entity</i>	<i>Purpose for which information is shared</i>	<i>Specific information types that are shared</i>	<i>Method of transmittal or disclosure</i>	<i>Safeguards for data transmittal and disclosure</i>
<i>EX: Company Q</i>	Insurance verification	Name, Personal Address, Social Security Number	Data is transferred via a secure file transfer every 3 months.	Data is sent via a secure one way file transfer using File Transfer Protocol.

4.4 What agreements, and other types of documentation, are in place, which establish parameters around the internal data sharing listed above, and how frequently are these documents reviewed?
<i>Examples: Memorandum of Agreement or Memorandum of Understanding (MOA/MOU) between Agency and Entity is reviewed annually. Contract XYZ is reviewed every three years.</i>

--

Section 5.0 Notice to Individuals to Decline/Consent Use

5.1 How is notice provided to the individual prior to the collection of information? If notice is not provided, explain why. Include the links to any web-based Privacy Policy or Notice.

Providing notice is the method by which an individual is informed of how his or her information will be used. Notice is provided prior to the collection of the individual's information. Please refer to the specific federal and/or State law, regulation, and/or Agency policy that applies to the collection of information from individuals.

--

5.2 Are individuals allowed to decline to provide information?

- Yes (Complete Question 5.3)
- No (Complete Question 5.4)

5.3 If individuals ARE allowed to decline to provide information, how are any resulting consequences, e.g., the State's inability to provide the service, explained to the individual?

--

5.4 If individuals are NOT allowed to decline to provide information, is notice of the collection of information provided to the individual? If notice is not provided, please provide detailed justification.

--

5.5 Are individuals informed of their right to consent to particular uses of the information (if applicable)? If so, how does the individual exercise that right?

--

--

Section 6.0 Individual Requests for Access, Redress, and/or Correction

6.1 What are the procedures that allow an individual to request access and/or to correct the information the Agency has collected regarding his or her information? How are individuals informed of this process?

6.2 Is there a way for an individual, who is dissatisfied with the Agency's initial response to his or her request for data access or correction, to ask for a review of the decision? If so, describe the process.

Section 7.0 Access Privileges and Security

7.1 What criteria are in place to determine which users or roles may access the Agency data records? Where are the procedures for requesting and modifying access privileges documented?

7.2 Do contractors have access to the Agency data records? If yes, describe privacy-related safeguards and requirements built into the contract language. <i>Examples of privacy safeguards may include: certification of privacy training prior to data access; non-disclosure or confidentiality agreements; background checks; and data breach reporting and notification responsibilities, etc.</i>

7.3 How are persons, who are given access to this data set, made aware of privacy safeguards?

--

7.4 Have the appropriate controls been implemented in accordance with the State Information Security Program (SC DIS 200 Standard 1.400)? Has the designated Agency manager documented his/her decision to accept any identified risks (SC DIS Control 4.205)?

--

7.5 What physical, administrative, and technical controls are in place to protect the data from unauthorized access and misuse? *Please describe the Physical, Technical, and Administrative Controls currently in place to account for and secure the PII.*

--

Appendix C
PTA/PIA Findings and Mitigation Plan Template

Business Process: _____

PTA/PIA#: _____

Privacy Threshold Analysis/Privacy Impact Assessment Findings and Mitigation Plan

Agency Name: _____

Agency Privacy Liaison: _____

Findings from Privacy Threshold Analysis (PTA)

Does this business process involve PII? Yes No

(If yes, complete the Privacy Mitigation Plan below.)

Privacy Mitigation Plan						
Risk #	Description of Privacy Risk	Planned Mitigation Action	Person Responsible for Mitigation Action	Projected Completion Date	Status*	Comments
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						

*Status: OT = On Target C = Closed D = Delayed