NCDIT | NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Privacy Threshold Analysis/Privacy Impact Assessment User Guide

User Guide for State Agencies

Version 1.0

August 10, 2026

Document Information

Revision History

Date	Version	New or Revised Requirement	Description	Author
Aug. 10, 2026	1.0	New	Standard Creation	Deborah Olagunju

Document Details

Department Name	Office of Privacy and Data Protection
Owner	
Title	State Agency Privacy Threshold Analysis/Privacy Impact Assessment User Guide
Publication Date	Aug. 10, 2026
Next Release	
Document Type	User Guide
Document Number	
Version	1.0

Table of Contents

Purpose

The purpose of this user guide is to assist state employees in understanding and maneuvering through the ServiceNow platform to submit Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA) forms.

Virtual training is also available through the NC Learning Center and is assigned, as needed, to employees.

Content Lead

N.C. Department of Information Technology, Office of Privacy and Data Protection

Definitions

Owner

The owner is the individual listed as the agency's Privacy Liaison. This role oversees, reviews, and can complete the Privacy Threshold Analysis/Privacy Impact Assessment

Parent Entity/Agency

The Parent Entity/Agency is the agency that is submitting the Privacy Threshold Analysis/Privacy Impact Assessment.

Privacy Threshold Analysis

A Privacy Threshold Analysis serves as the document used to identify information technology (IT) systems, technologies, rulemaking, programs, information sharing arrangements, or pilot projects that involve public and personal data, and other activities that otherwise impact the privacy of individuals as determined by the N.C.G.S. 132-1.10.

Privacy Impact Assessment

A Privacy Impact Assessment is an analysis of how information is handled to:

i) Ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy.

ii) Determine the risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of information in identifiable form in an electronic information system.

iii) Examine and evaluate protections and alternate processes for handling information to mitigate potential privacy concerns. A privacy impact assessment is both an analysis and a formal document detailing the process and the outcome of the analysis.

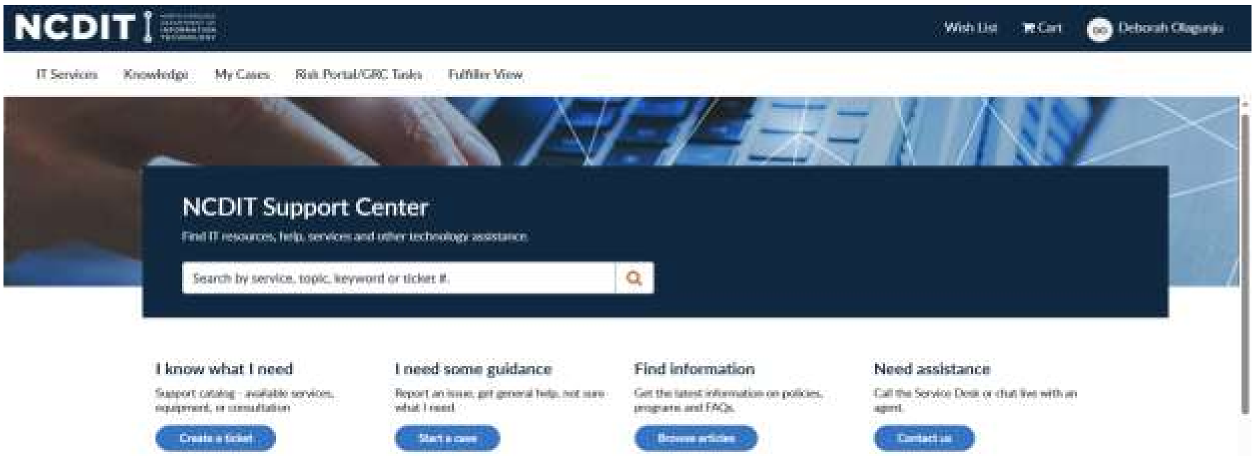
Program Manager

The Program Manager is the individual completing the Privacy Threshold Analysis/Privacy Impact Assessment. Generally, the Program Manager can be the owner or an individual on the project's team assigned to complete the Privacy Threshold Analysis/Privacy Impact Assessment. This role can be reassigned throughout the Privacy Threshold Analysis/Privacy Impact Assessment process.

Accessing the Privacy Threshold Analysis

Accessing the PTA from the Governance and Risk Compliance (GRC) Portal

1. Enter https://ncdit.servicenowservices.com/ncditsupport in your browser's search bar.

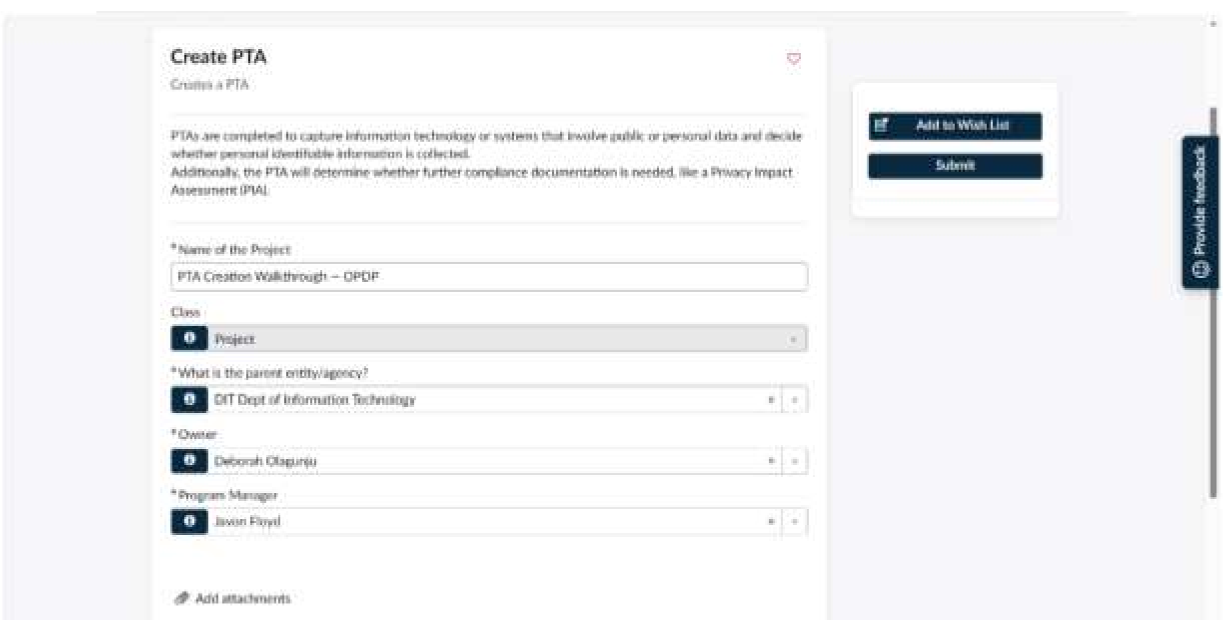


2. Type **Create PTA** in the NCDIT Support Center search bar.

3. Enter the name of the project, the agency, owner (i.e., the agency privacy liaison), and the program manager in the respective spaces. See the example below.

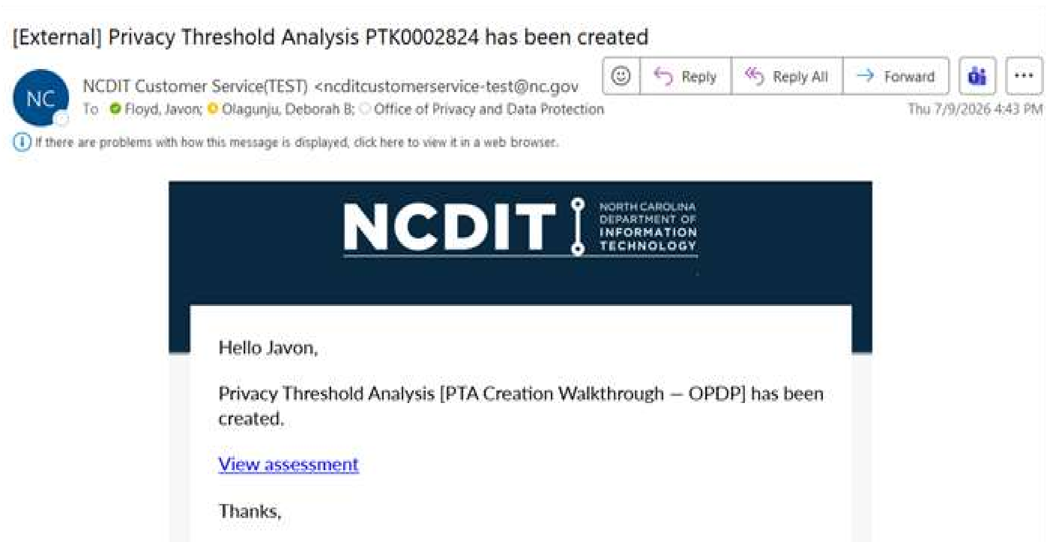
   Key takeaways:

   - The **Owner** will be the privacy liaison for the agency.
   - The **Program Manager** is the individual completing the PTA. (Please note that the privacy liaison can also be the program manager.)

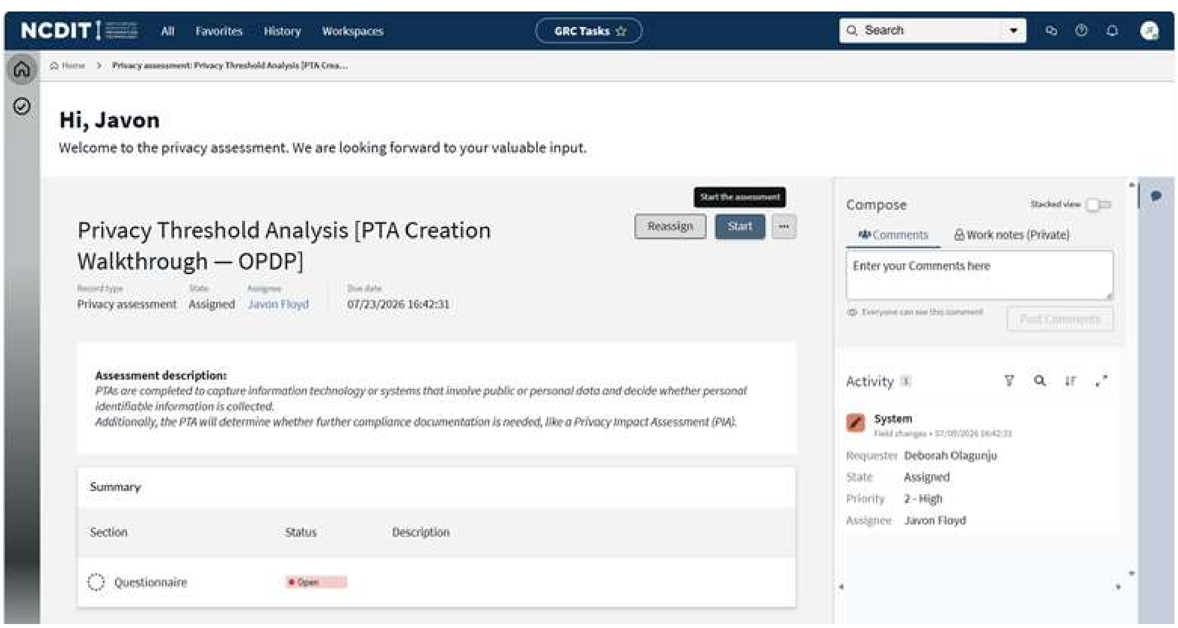


4. Press **Submit**.

5. **Two** email notifications from **NCDIT Customer Service** will populate to the accounts listed in the **Owner, Program Manager, and Office of Privacy and Data Protection**.
    a. The first email will inform all parties that a PTA has been created.
    b. The second email will provide a link to the PTA.
6. Click the **View assessment** link in the email.

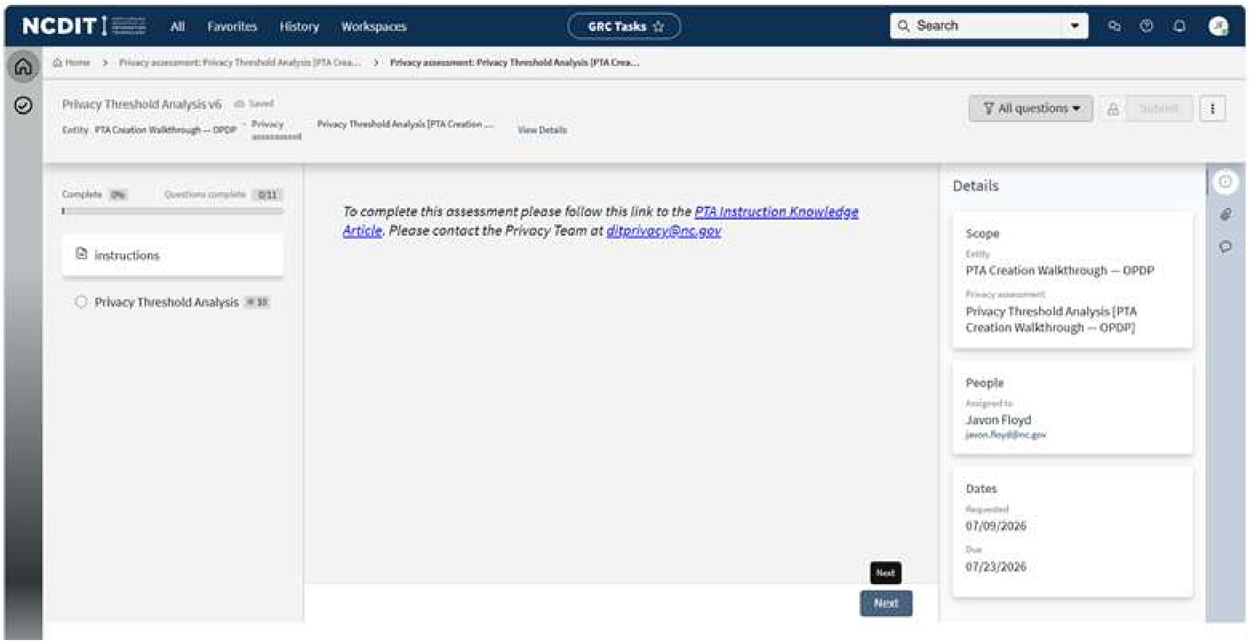


7. Once the privacy assessment page opens, review the assessment description.
8. Click **Start** to begin the PTA form.

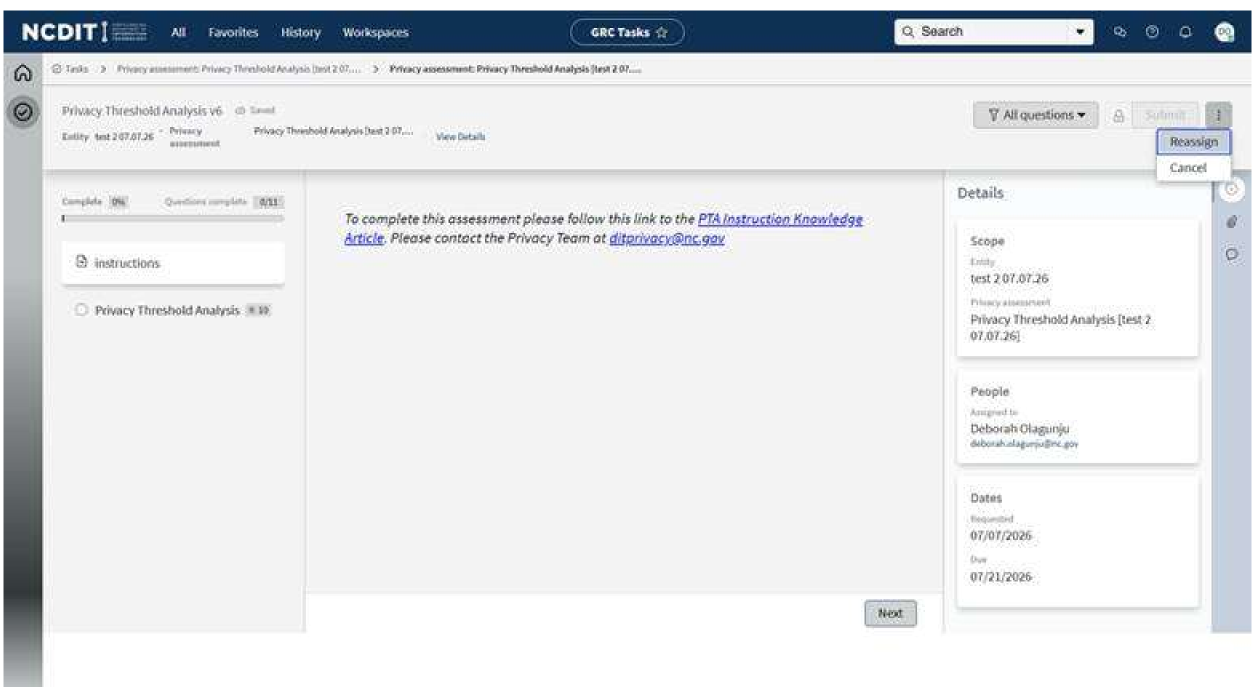


9. Users can review the PTA Instruction Knowledge Article to understand the purpose of the PTA.

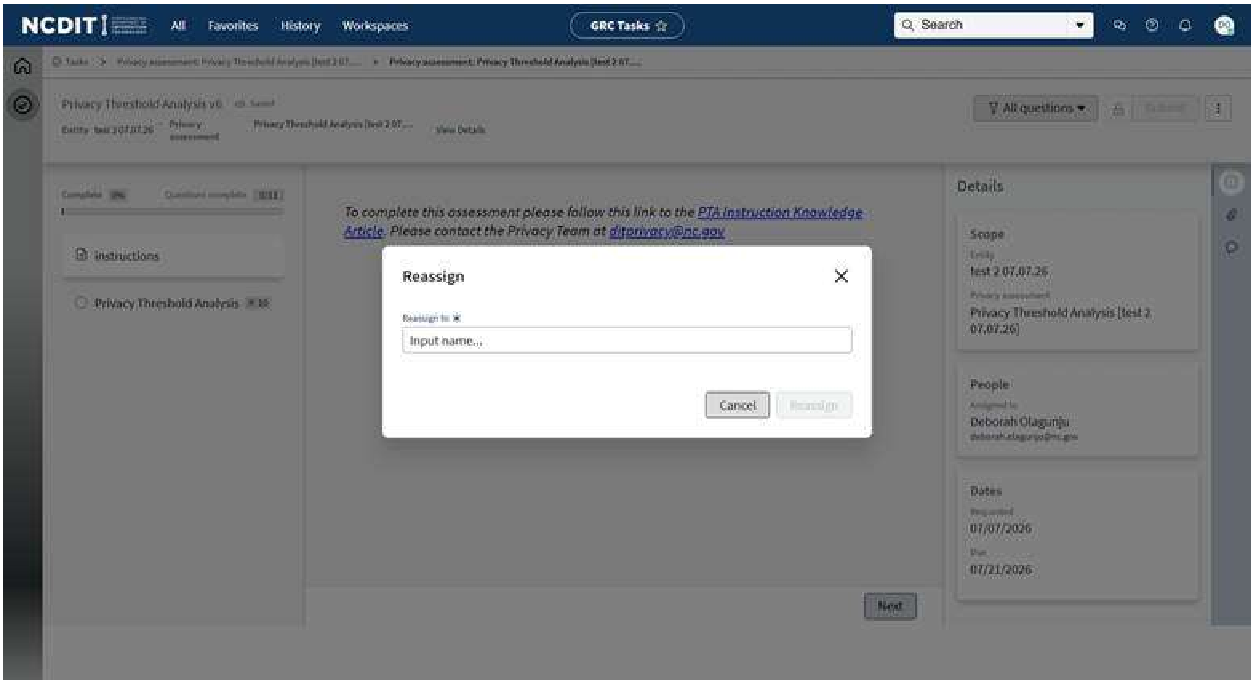
10. Click **Next** to start the PTA form.



11. In the event an agency wants to reassign completion of the PTA to another team member, click the three dots on the **TOP RIGHT** of the page. Click **Reassign**.



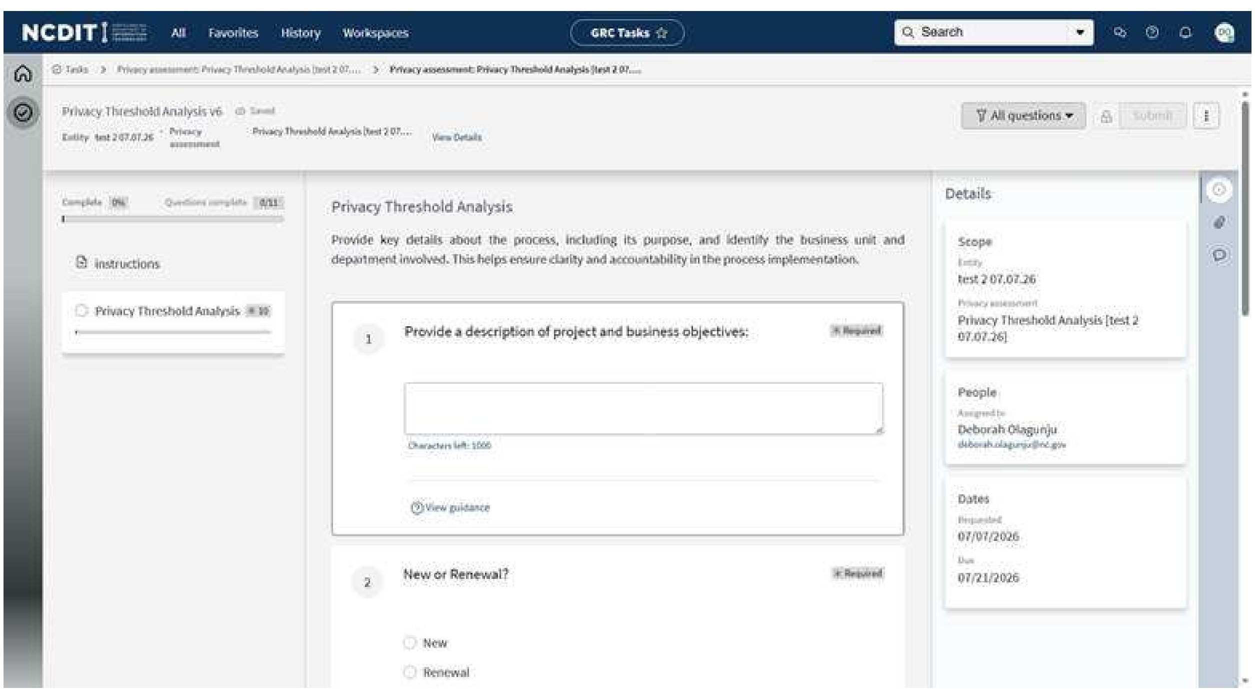
12. Type the **First and Last name** of the user and click **Reassign**.

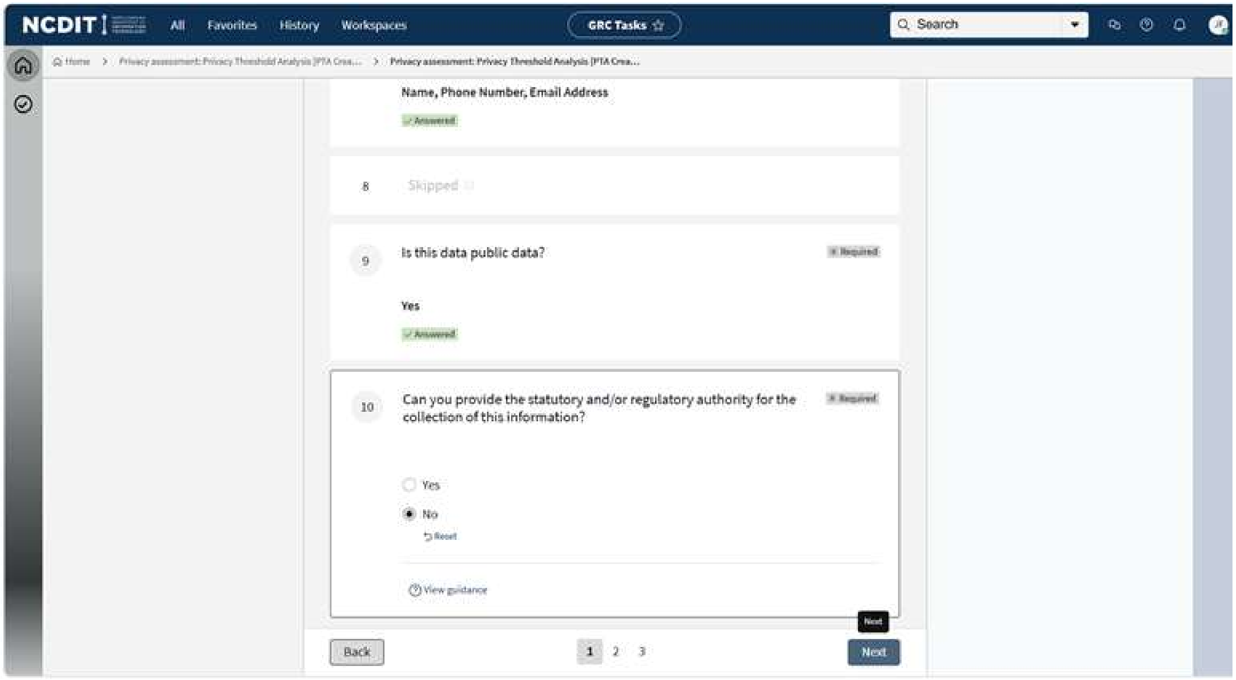


13. An email notification will be sent to the Assignee and the Assignor. The Assignee will be able to complete the PTA by clicking **View assessment** in the email.

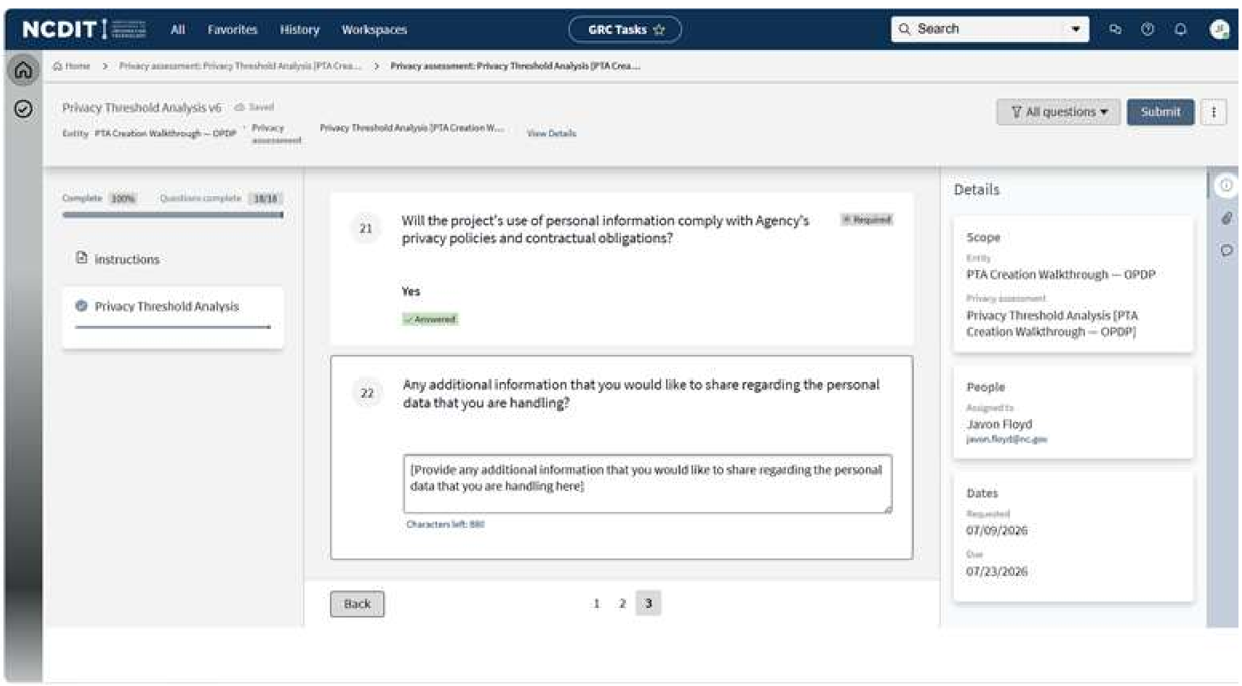
Privacy Threshold Analysis Assigned

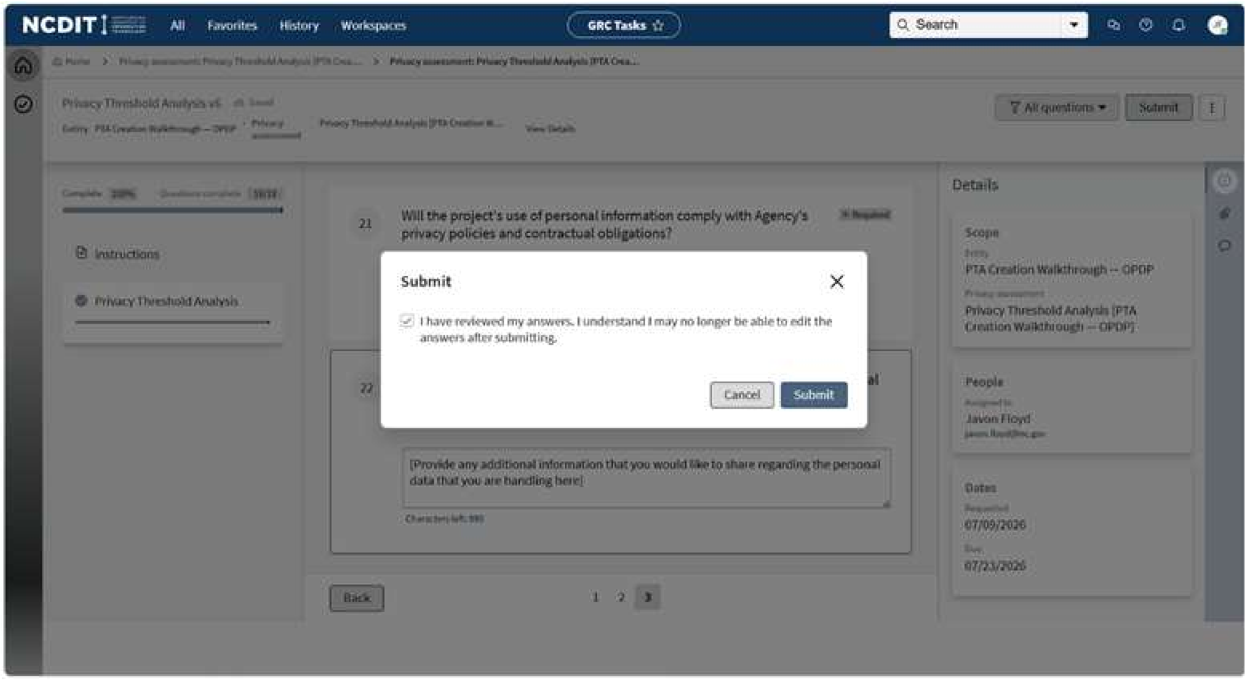
1. Complete the PTA questions. For a list of questions contained in the PTA, refer to the section in this document called [Privacy Threshold Analysis Questions](#).





2. Once completed, click the **Submit** button at the top right section of the page. Then, **check the box**, and click **Submit**.





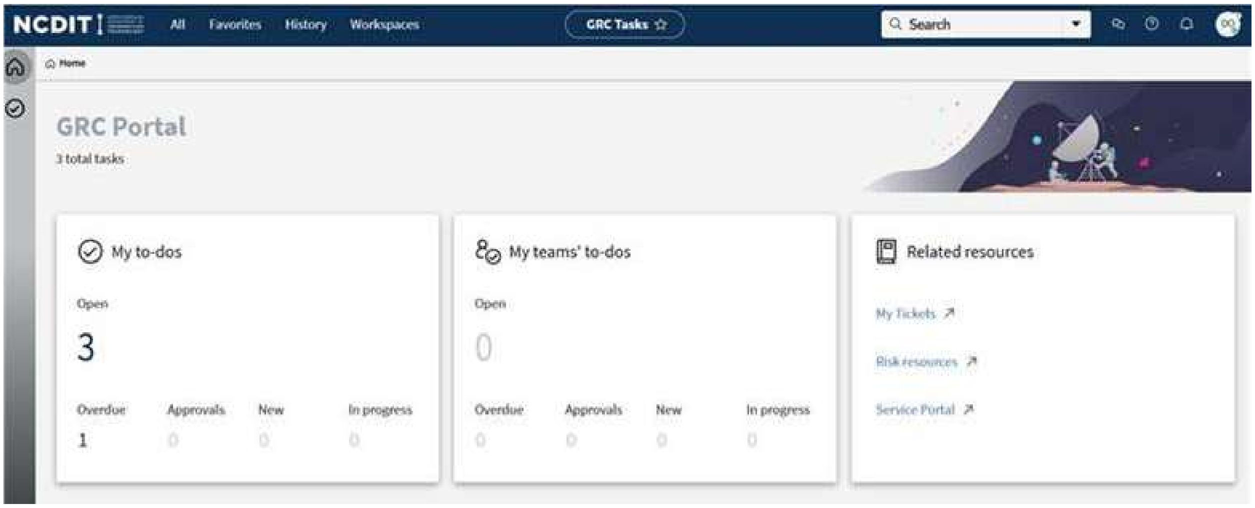
Accessing the PTA/PIA Through Risk Portal/GRC Tasks

After creating the PTA/PIA, a task will populate within the user's portal. To locate the task:

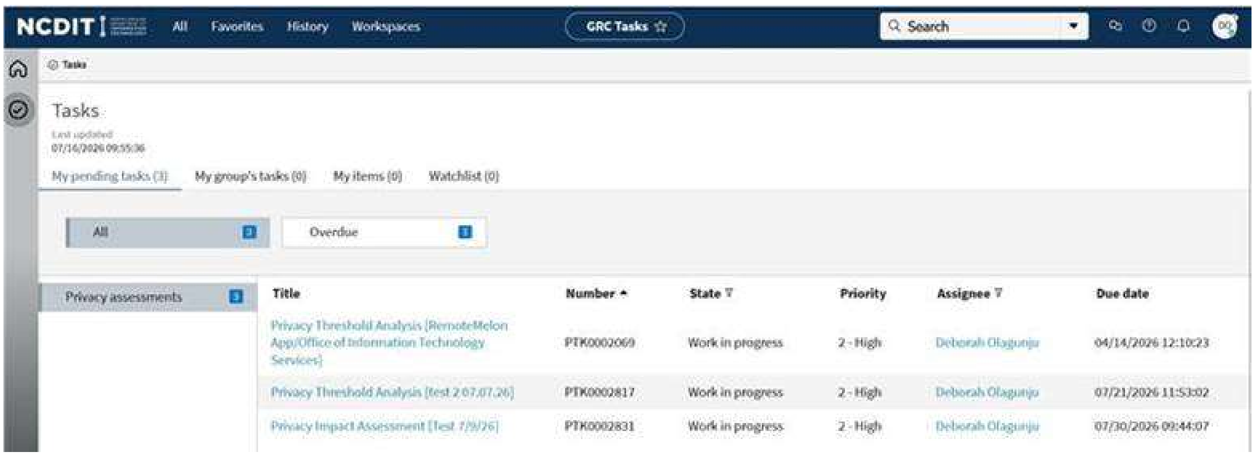
1. Click **Risk Portal/GRC tasks** in the navigation bar at the top of the page.

2. In the **Governance and Risk Compliance (GRC) Portal**, under **My to-dos** click **the number** under **Open**.

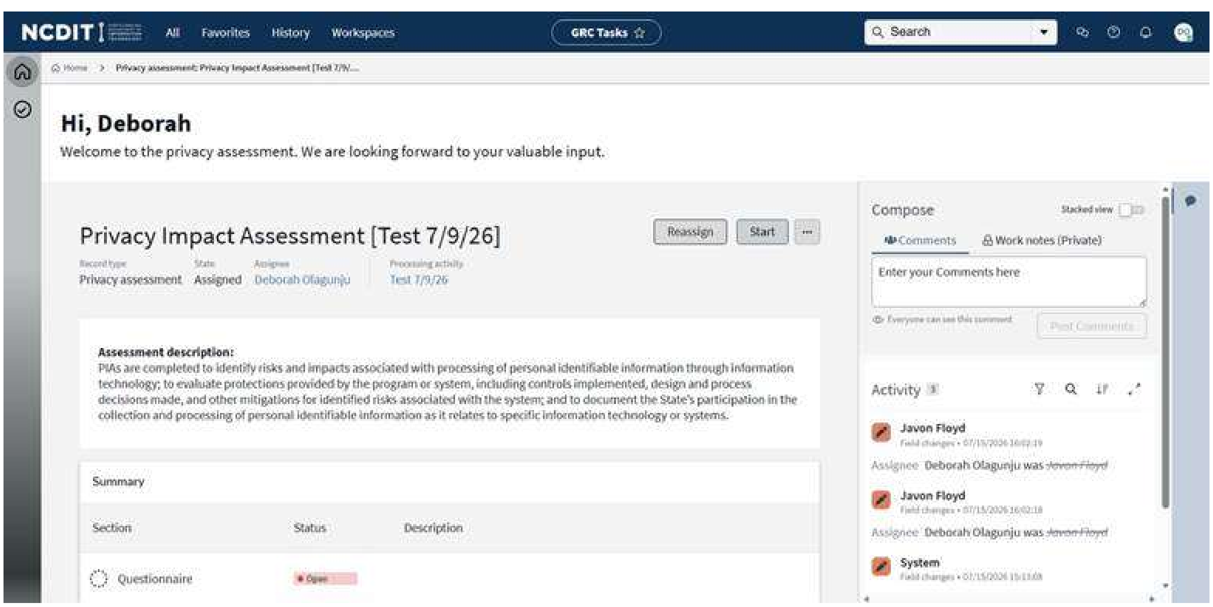
   For example, in the image below, you would click **3** in the **My to-dos** section.



3. Find the **Privacy Threshold Analysis** or **Privacy Impact Assessment** in your pending tasks.

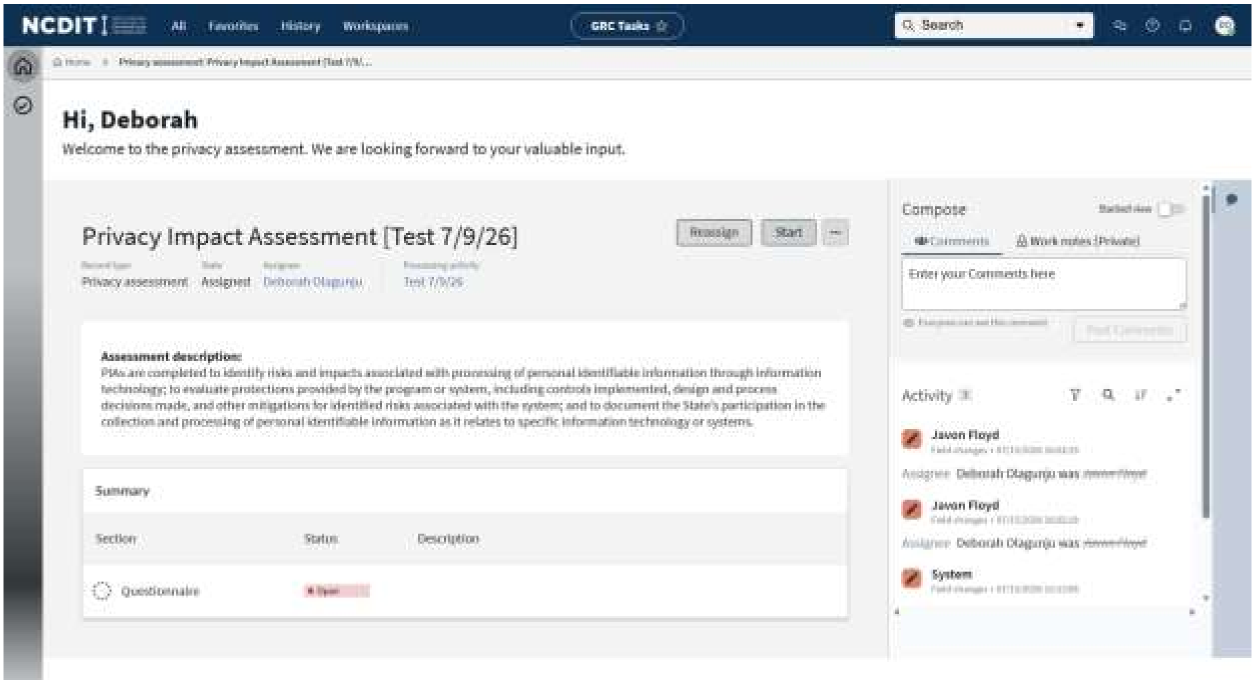


4. Once you click on the PIA, select **Start** and **complete the PIA**.



Accessing the Privacy Impact Assessment (PIA)

Once the PTA has been reviewed and approved by the Office of Privacy and Data Protection, an email notification will be sent to the assignee and assignor of the PTA. This email will contain the link to the Privacy Impact Assessment (PIA). Click the **View assessment** link in the email, and the link should open to the PIA page.

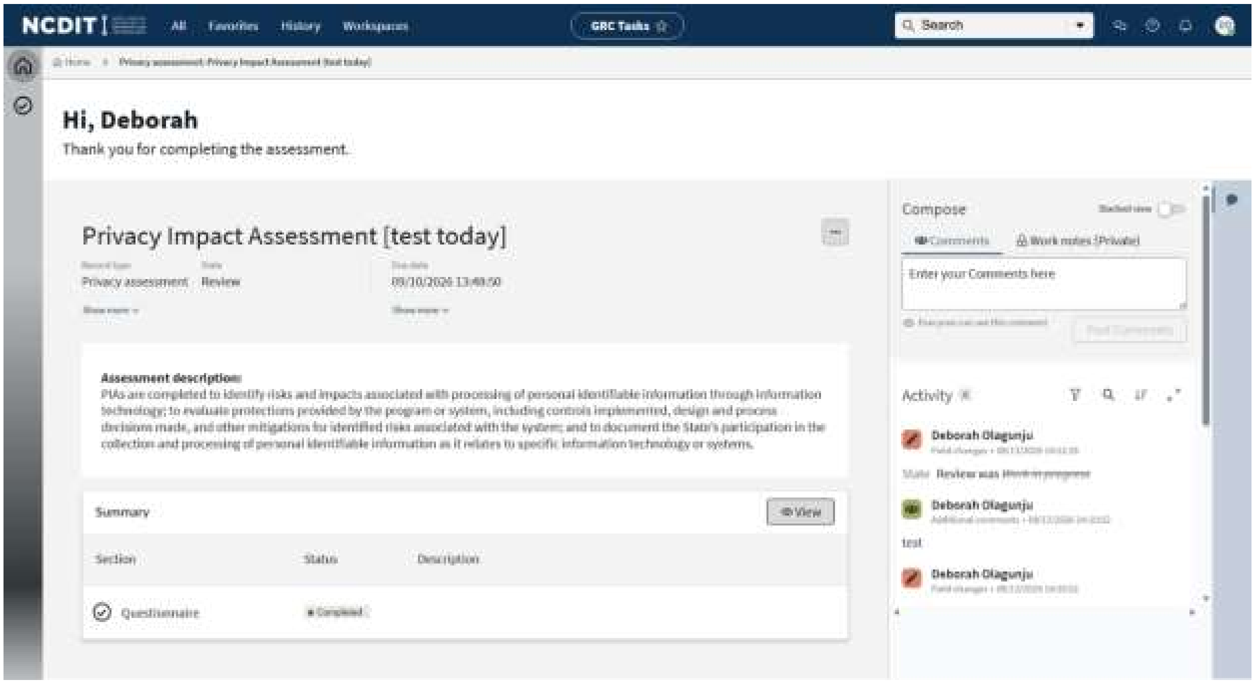


In the event, users do not receive an email notification, they can access the PIA from the Risk Portal.

For more information, refer to the section earlier in this document called Accessing the [PTA/PIA Through Risk Portal/GRC Tasks].

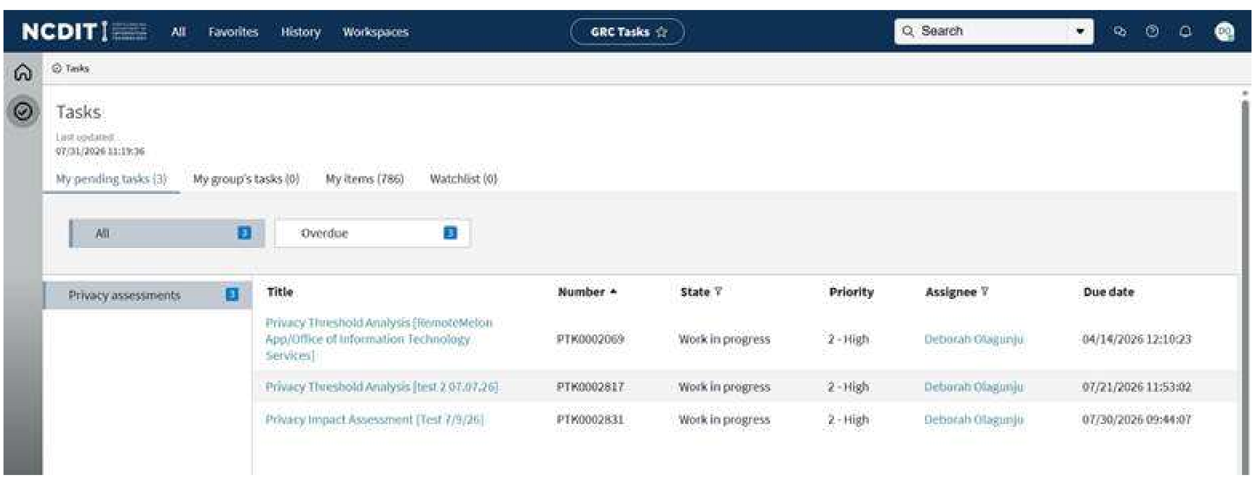
Request for Revision

After the Office of Privacy and Data Protection completes its review of a PTA or PIA, additional information or clarification may be requested. If so, users will receive an email prompting them to revise their submission. Details about the revision request can be found in the activity section of the assessment page.



Locating Submitted PTAs/PIAs

Once your PTA/PIA is submitted, you can locate them in the Tasks folder. Here, you can find all PTA/PIAs assigned to you or your agency. You will be able to identify how many have been reviewed, approved, or subsequently denied.



Privacy Threshold Analysis Questions

The Office of Privacy and Data Protection has listed below the questions in the Privacy Threshold Analysis. The purpose is to help agencies understand the intention of the question and the information we need to receive to review and subsequently approve their request.

Question 1
Provide a description of project and business objectives.

Rationale: We are looking for a highlight explanation of why the agency is seeking to use the project, tool or system and how it fits into the business objectives.

Question 2
New or Renewal?

Rationale: If this is a renewal to a PTA, Question 3 will trigger, asking for the number of the previous PTA.

Question 3
Project or PTA ID Number for Renewal

Question 4
Will the data collected contain personal information?

Rationale: If the answer is Yes, Question 5 will trigger.

Question 5
Whose personal information will be collected, shared, used, or stored by the project?

- Members of public/constituents
- State employees/contractors
- Third parties (i.e. vendors, partners
- Others (incarcerated individuals, minors, for research purposes)

Rationale: If the answer is Other, Question 6 will trigger.

Question 6
Please detail whose personal information will be collected, shared, used, or stored by the project.

Question 7
Which types of information will the project collect, share, use, or store?

- Name
- Social Security Number
- Financial Account Number
- Location Data
- Phone Number
- Email Address
- Race / Ethnicity
- Driver's License
- Physical Address
- Family or Marital Status
- Photo or Video
- Gender
- Account Number
- Biometric Data
- Other (please specify in the question below)

Rationale: If the answer is Other, Question 8 will trigger.

Question 8

Please detail the types of information collected.

Question 9
Is this data public data?

- Yes
- No

Question 10
Can you provide the statutory and/or regulatory authority for the collection of this information?

Question 11
Approximate number of individuals affected (estimate over project lifetime)?

Question 12
To the best of your knowledge, is this the first time the personal information will be used, shared, or stored in this way by your agency?

Question 13
Will personal information be shared with third parties?

- Yes
- No

Question 14
Will the project employ the use of new technology not currently used at your agency to collect, store, use, or share personal information?

- Yes
- No

Question 15
Where will personal information be stored?

- Agency-hosted
- State cloud
- Third-party cloud/on-prem/hybrid
- Paper
- Mobile device
- Other

Rationale: If the answer is Other, Question 15 will trigger.

Question 16
Please provide information regarding where the personal information will be stored.

Question 17
From which jurisdiction will the project collect personal information

- US
- Canada
- EU
- Multiple Jurisdictions
- Other

Question 18
Does the process/product process data concerning vulnerable individuals (data subjects including children, mentally ill persons, asylum seekers, elderly, patients)?

Question 19
Will the information retention period for this project comply with agency's record retention schedule?

Question 20
Does the system employ artificial intelligence?

- Yes
- No

Question 21
Will the project's use of personal information comply with agency's privacy policies and contractual obligations?

Question 22
Any additional information that you would like to share regarding the personal data that you are handling?

Privacy Impact Assessment Questions

The Office of Privacy and Data Protection has listed below the questions in the Privacy Impact Assessment. The purpose is to help agencies understand the intention of the question and the information we need to receive to review and subsequently approve their request.

Question 1
Describe the purpose and functionality of the system/project being assessed, including its users and core workflows.

Rationale: We need clarity around what the system does, its interactions, and how data flows across the core processes.

Sample Answer: The system is designed to streamline the collection, processing, and management of operational data related to agency activities.

Question 2
Approximate number of unique individuals whose personal data will be processed by this system or tool.

Rationale: We need to understand the number of individuals affected to determine the scale of privacy risk and the compliance standards for data minimization and proportionality principles.

Question 3
Number of employees assigned to support the information technology in scope for this PIA.

Question 4
What is the relationship between the agency or department and the individual (select all that apply)?

- Resident
- Website visitor
- Employee
- Contingent Worker (3rd Party)
- Strategic Partner (3rd Party)
- Other (please describe on the next question)

Question 5
Specify the range of users whose data is stored as part of this process.

Question 6
Please select the approximate age range of the individuals' personal data which will be processed by the IT system. (Select all that apply.)

- < 13 years of age
- 13 - < 18 years of age
- 18 - < 65 years of age
- 65 years of age or older

Question 7
How is personal data collected? (Select all that apply.)

- Directly from the individual
- Indirectly from a public source
- Indirectly from another government entity
- Indirectly from a non-government entity (3rd party)
- Other (please describe on the next question)

Question 8
Does your system or tool have any AI features or functionalities?

- Yes
- No
- Not Sure (please explain)

Question 9
If yes, please list all AI features and functionalities here.

Question 10
Please list all personal data and user data that is in scope for this PIA.

Question 11
What systems are being used to help with the collection, use, sharing, or storage of personal information?

Option to type response or upload attachment.

Question 12
Is the data state-hosted?

Question 13
As this tool handles sensitive personal information (PII), a justification of purpose is required. Explain the essential and proportional need for the processing of this specific sensitive data to achieve the project's objectives.

Question 14
Do you provide a privacy notice to individuals that is fully compliant with North Carolina's Department of IT's Statewide Privacy Policy and clearly states in plain language all intended purposes and uses of the personal data; the consequences for refusing to provide the personal data; the classes of persons and governmental entities with whom the governmental entity shares personal data?

- Yes
- No
- N/A (please explain)

Question 15
If you meet the criteria in North Carolina's Department of IT's Statewide Privacy Policy, the privacy notice may be posted on the public notice website otherwise it must be posted on the governmental entity. Where is your privacy notice posted?

- Posted on the public notice website
- Not posted on the public notice website

Question 16
If posted on the public notice website, the CIO is attesting to the fact the government entity does not have a government website. Provide a link to the posting on the public notice website as evidence.

Question 17
Will the system or tool use personal data you previously obtained but is being used for a new purpose?

- Yes
- No
- Not Sure (please explain)

Question 18
What is the purpose for processing the personal data? (Select all that apply.)

- **Audits and Inspections:** *Verifying compliance with standards, laws, and policies.*
- **Cultural Preservation:** *Maintaining archives, libraries, and museums.*

- **Crisis Communication:** *Providing updates and information during emergencies or disasters.*
- **Digital Identity and Authentication:** *Enabling access to government services through digital platforms.*
- **Economic and Social Research:** *Understanding trends to design economic and social interventions.*
- **Education Administration:** *Managing student records, attendance, and performance data.*
- **Elections and Democratic Processes:** *Voter registration, election management, and vote processing.*
- **Emergency Response:** *Coordinating disaster relief and public safety in emergencies.*
- **Employment and HR Management:** *Managing government employee records, payroll, pensions, and benefits.*
- **Fraud Prevention and Detection:** *Identifying and mitigating fraudulent activities in public programs and benefits.*
- **Identity and Citizenship Management**: *Issuing IDs, driver's licenses, and maintaining birth, marriage, and death registries.*
- **Infrastructure Development:** *Managing transportation, utilities, and urban planning.*
- **Law Enforcement and Public Safety:** *Criminal investigations, maintaining public safety, and enforcing laws.*
- **Licensing and Permitting:** *Granting business, construction, and other permits or licenses.*
- **Policy Development and Evaluation:** *Analyzing data to inform policy decisions and program improvements.*
- **Public Consultation and Participation**: *Engaging citizens in policymaking, surveys, or town hall meetings.*
- **Public Health Management:** *Managing pandemics, monitoring disease outbreaks, and providing vaccinations.*
- **Public Service Delivery:** *Providing essential services such as healthcare, education, social services, and housing.*
- **Regulatory Oversight:** *Enforcing laws and regulations in areas like environmental protection, financial regulation, and consumer rights.*
- **Subsidy and Benefit Distribution**: *Allocating financial support for eligible citizens or businesses.*
- **Taxation and Revenue Collection:** ***Collecting*** *and managing taxes, fees, and other government revenues.*
- **Transparency and Accountability**: *Responding to public records requests and ensuring government accountability.*
- **Website and Service Analytics:** *Monitoring and improving government websites and e-services.*
- **Worker and Public Safety:** *Monitoring and promoting workplace and public safety standards.*
- **Other (please describe):**

Question 19

Do you collect more personal data than is reasonably necessary to efficiently achieve the specified purposes identified above?

- Yes
- No

Question 20

If you collect more personal data than is reasonably necessary, please describe the specific personal data you collect that is not reasonably necessary. If your entity has a minimization plan to dispose of the personal data which is not necessary, please describe.

Question 21

Describe your methodology for ensuring the accuracy and completeness of the personal data collected.

Question 22

Is your agency or department sharing the personal data described in this PIA?

- Yes
- No

Question 23

Do you maintain a list of the names and contact information for the partners with whom you share information?

- Yes
- No

Question 24

Who is the personal data shared with? (Select all that apply.)

- Governmental entity
- Non-governmental entity

Question 25
Describe the intended use of the personal data by the other party.

Question 26
Provide a note as to the length of time your entity is obligated to share the personal data.

Question 27
Describe the final disposition of the data shared with the other entity when the sharing agreement terminates.

Question 28
Does your department or agency have any agreements with third parties to process personal data within the scope of this PIA?

- Yes
- No
- Not Sure (please explain):

Question 29
If yes, please provide the storage location where the information is. List what personal data elements are processed with the external entity.

Question 30
Do you include in your contract standard terms and conditions the requirements for contractors contained in North Carolina's Department of IT's Statewide Privacy Policy?

- Yes
- No
- Not Sure

Question 31
Where is the personal data stored? (This should correspond with the data maps you have provided above.)

- On-premises
- Third Party Cloud Provider
- Hybrid Solution

Question 32
For any personal data not stored on-premises, do you have legal agreement with third-party providers that ensure no State-owned data is stored or processed outside the continental United States?
Options:

- Yes
- No
- Not Sure

Question 33
Do you have an incident response plan with a breach notification plan?

- Yes
- No
- Not Sure (please explain)

Question 34

Do you have defined access control procedures?

- Yes
- No (Contact ESRMO)
- Not Sure (please explain)

Question 35

Explain the procedure for removing access to this information for employees who have left your agency or department, individuals who no longer require access or who are no longer with the third-party.

Roles and Responsibilities

N.C. Department of Technology's Privacy Liaison, Program Managers and additional team members are responsible for initiating and overseeing the lifecycle of all PTAs and PIAs.

The Office of Privacy and Data Protection is solely responsible for reviewing and approving all submitted PTAs and PIAs.

Review Cycle

This Privacy Threshold Analysis/Privacy Impact Assessment User Guide will undergo a periodic review at annual intervals, or as changes are required. Updates to the guide will be determined based upon the nature of the policy and requirements driven by need.

Any identified changes, or outdated information within the policy will be addressed promptly. This may involve revisions, additions, or removals as needed to ensure that policies remain current and relevant.

The following roles provide leadership and management over this policy in accordance with the NCDIT Policy Management Policy:

- State Chief Information Security Officer (SCISO)
- Chief Privacy Officer

References

Statewide Privacy Threshold Analysis & Privacy Impact Assessment Procedure