WaTech
Washington Technology Solutions

Privacy Threshold Analysis

Integrating privacy into security review – March 2023

WaTech
Washington Technology Solutions

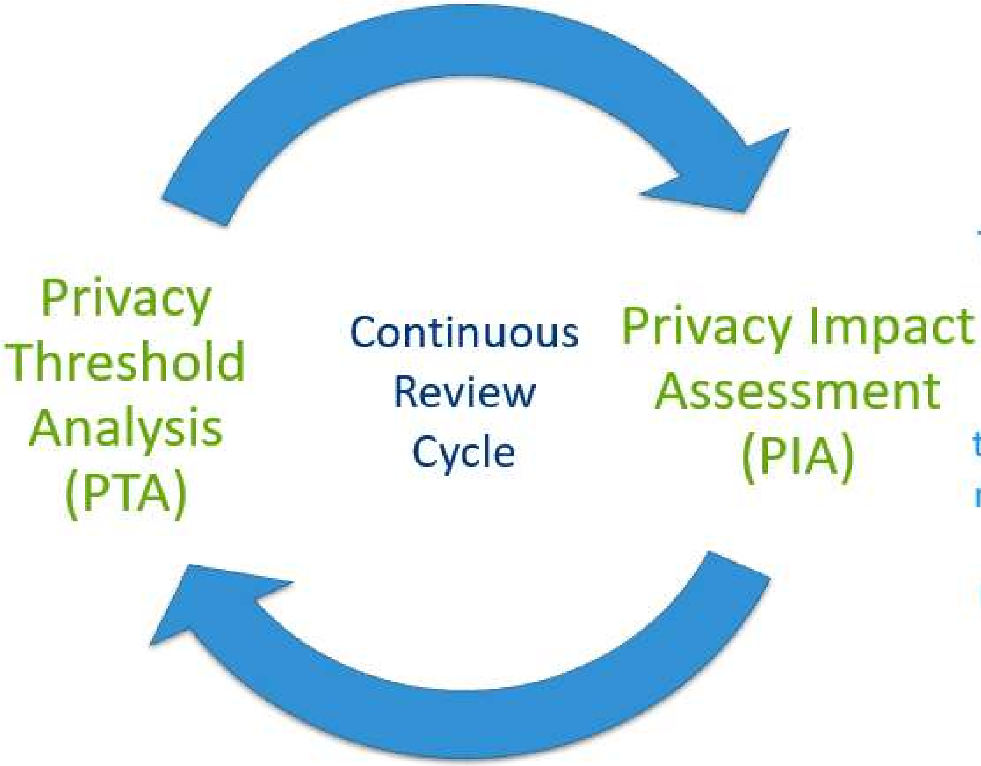
Today's agenda

- PTA and Privacy Impact Assessment overview
- The PTA process as part of security design review
- PTA completion tips
- Introduction to PIAs

WaTech
Washington Technology Solutions

PTA and PIA overview

A PTA is a brief, high-level assessment used to determine whether the subject of the review may have privacy implications and require a PIA.


Privacy Threshold Analysis (PTA)
Continuous Review Cycle
Privacy Impact Assessment (PIA)

The PIA is a tool designed to help consider how privacy principles have been incorporated into the project, assess privacy risks and how they should be appropriately mitigated, and document these findings.

Review and Update, as Appropriate

Preparation

- Ensure a clear understanding of the process and roles and responsibilities.
- Define the scope of the review.

PTA

- Provide a high-level description of the project and describe if PII is involved.
- Determine whether a PIA is required.

PIA

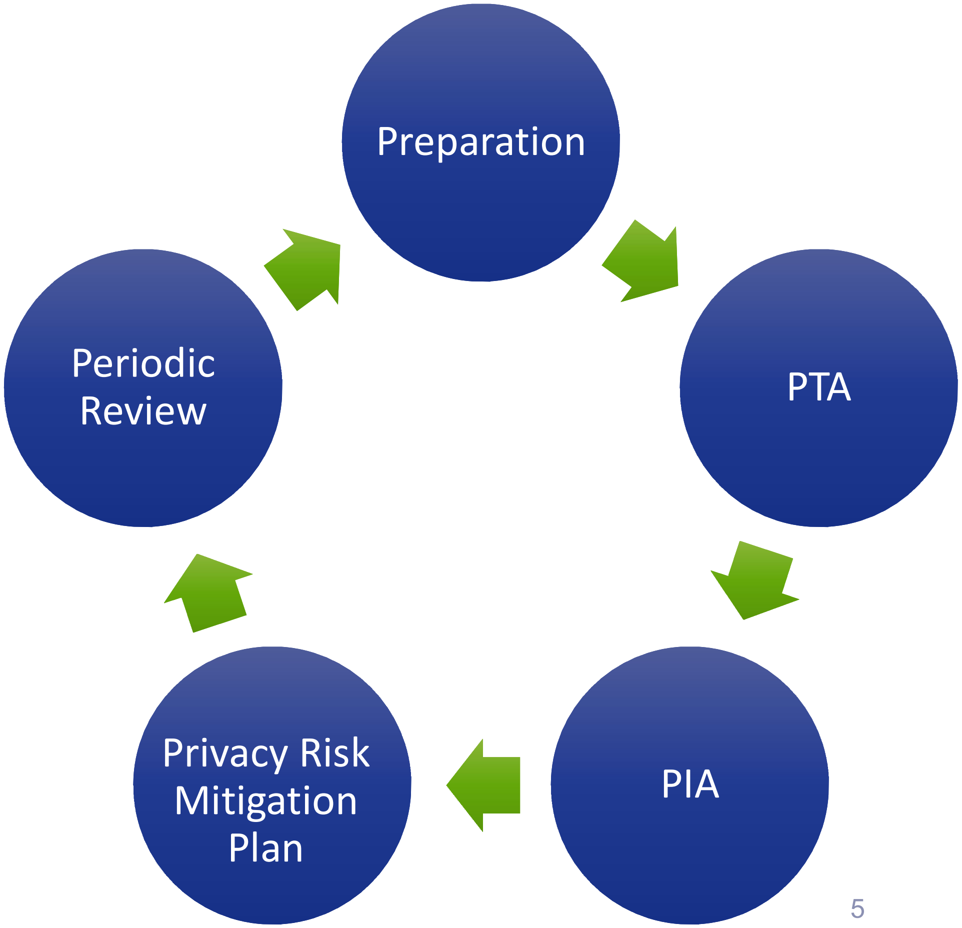
- Consider the Washington State Agency Privacy Principles.
- Document privacy risks and mitigation strategies.

Privacy Risk Mitigation Plan

- Clearly define how each mitigation strategy will be implemented.

Periodic Review

- Revisit past PTAs and PIAs.
- Update or replace, as needed.



Industry standards

E-Government Act of 2002

- Federal agencies must conduct PIAs

State privacy laws

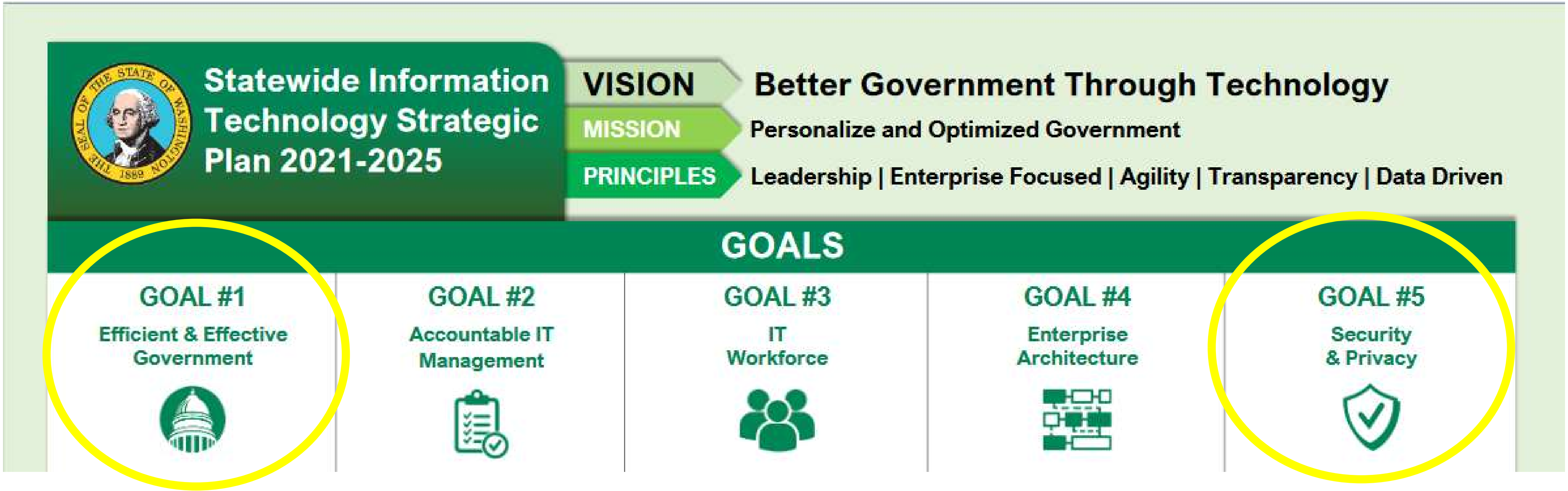
- Covered organizations (private sector) must conduct PIAs in certain circumstances in California, Colorado and Virginia
- Washington Privacy Act (not passed) would require covered organizations (private sector) to conduct PIAs in certain circumstances

Europe

- Organizations (private and public) must conduct PIAs

Key benefits

- Formalize a place for privacy consideration
- Shift left – be proactive, consider privacy when there is time to address risks
- Ensure consistency with applicable laws and privacy principles
- Expand perspective – consider privacy risks through lens of potential harm to constituents rather than harm to organization
- Decrease privacy risks / increase trust
- Improved collaboration – privacy is inherently multi-disciplinary and PIAs foster collaboration between business and technical teams



Statewide Information Technology Strategic Plan 2021-2025

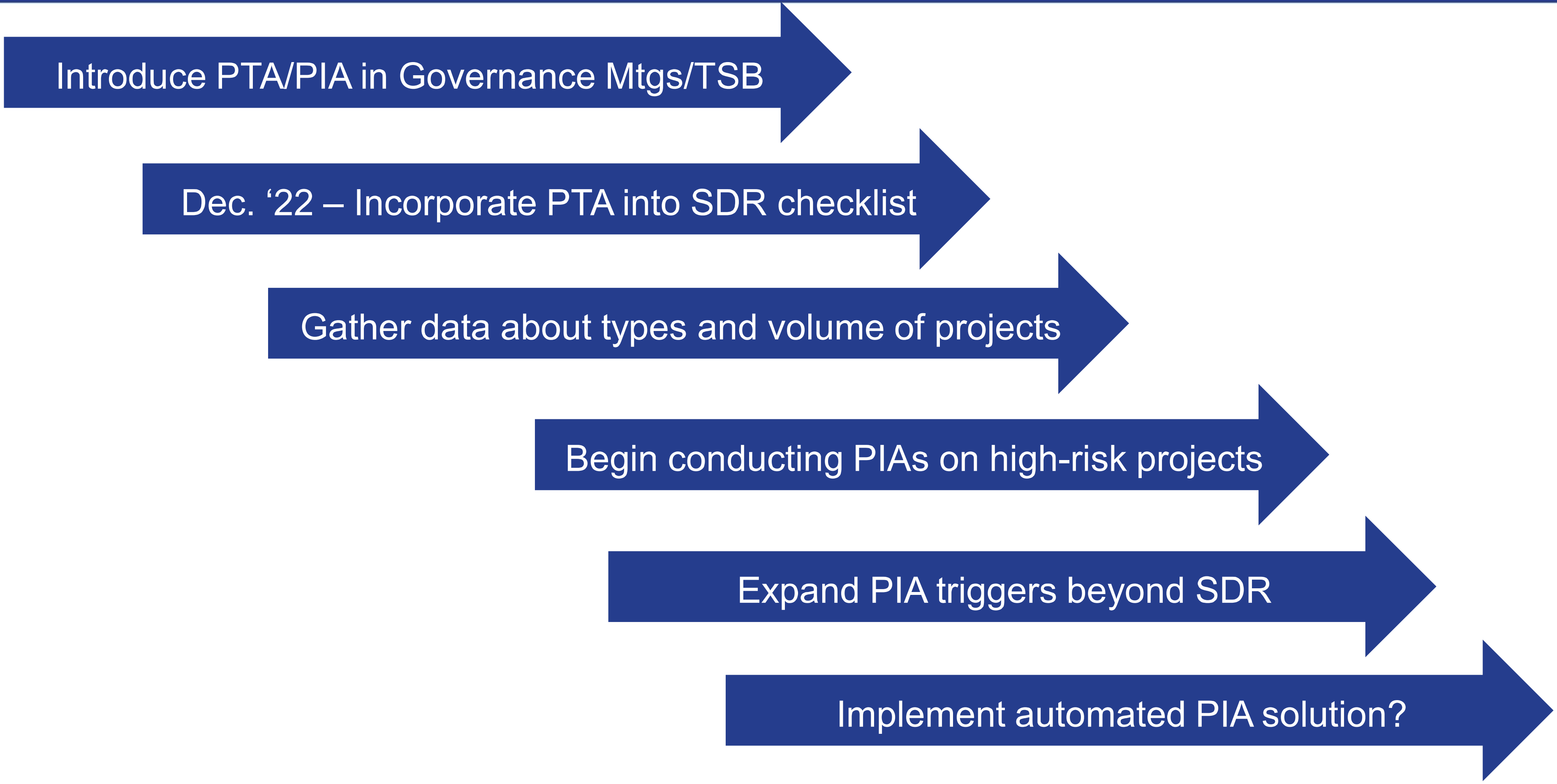
VISION Better Government Through Technology

MISSION Personalize and Optimized Government

PRINCIPLES Leadership | Enterprise Focused | Agility | Transparency | Data Driven

GOALS

GOAL #1	GOAL #2	GOAL #3	GOAL #4	GOAL #5
Efficient & Effective Government	Accountable IT Management	IT Workforce	Enterprise Architecture	Security & Privacy



Introduce PTA/PIA in Governance Mtgs/TSB

Dec. ‘22 – Incorporate PTA into SDR checklist

Gather data about types and volume of projects

Begin conducting PIAs on high-risk projects

Expand PIA triggers beyond SDR

Implement automated PIA solution?

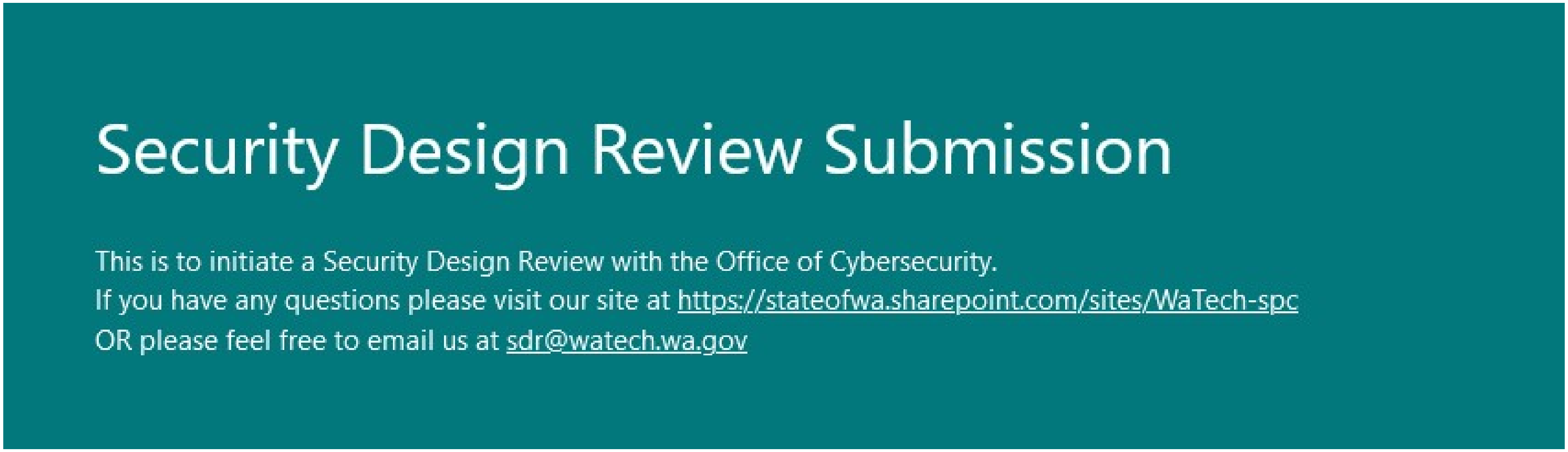
WaTech
Washington Technology Solutions

The PTA process

Ideal state

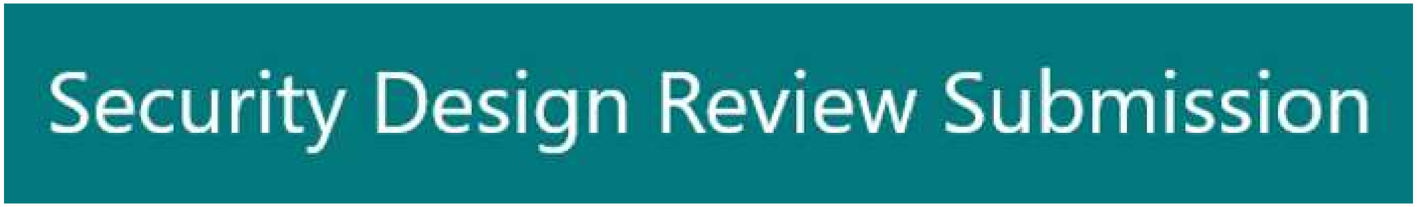
A PTA/PIA is conducted for business processes, systems, programs and technologies that involve PII.

- The process is initiated early in the development or procurement process for new projects.
- The process is initiated when there are substantive changes, such as:
  - Adding or merging data, changing technology solution, using new sources, sharing with new entities, changing data uses

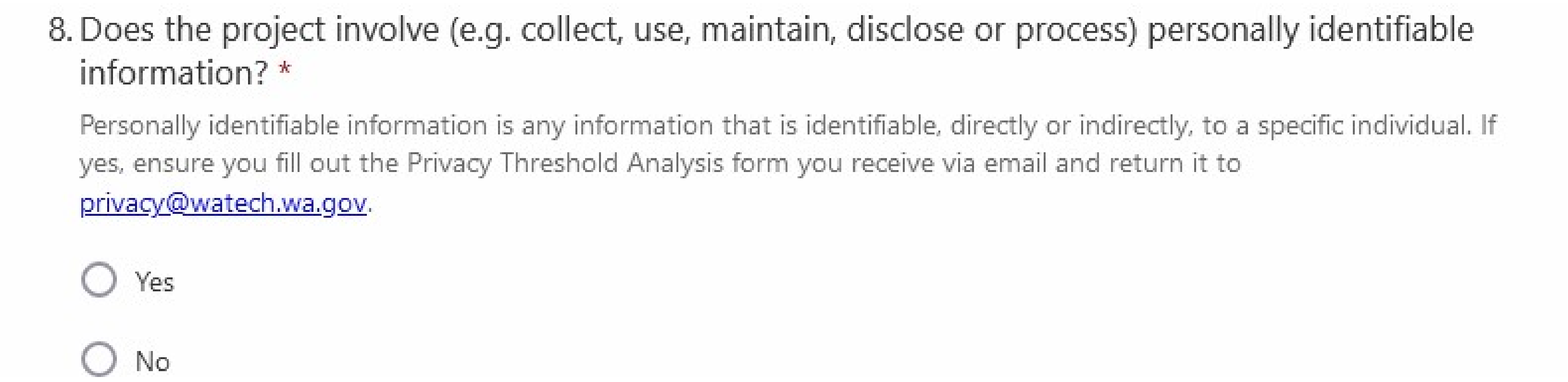


Security Design Review Submission

This is to initiate a Security Design Review with the Office of Cybersecurity.
If you have any questions please visit our site at https://stateofwa.sharepoint.com/sites/WaTech-spc
OR please feel free to email us at sdr@watech.wa.gov



Security Design Review Submission



8. Does the project involve (e.g. collect, use, maintain, disclose or process) personally identifiable information? *

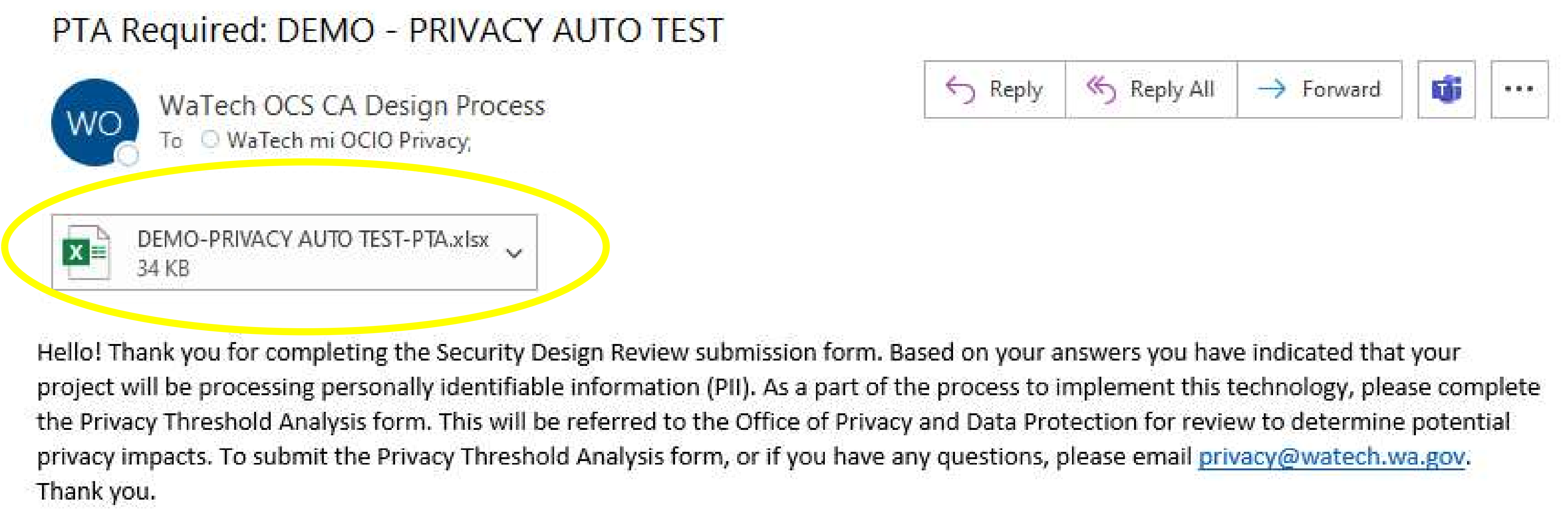
Personally identifiable information is any information that is identifiable, directly or indirectly, to a specific individual. If yes, ensure you fill out the Privacy Threshold Analysis form you receive via email and return it to privacy@watech.wa.gov.

○ Yes

○ No

Personally identifiable information (PII)

- Not just external customers
- Not just elements from RCW 42.56.590
- Not just Category 3 and 4 information



PTA Required: DEMO - PRIVACY AUTO TEST

WaTech OCS CA Design Process

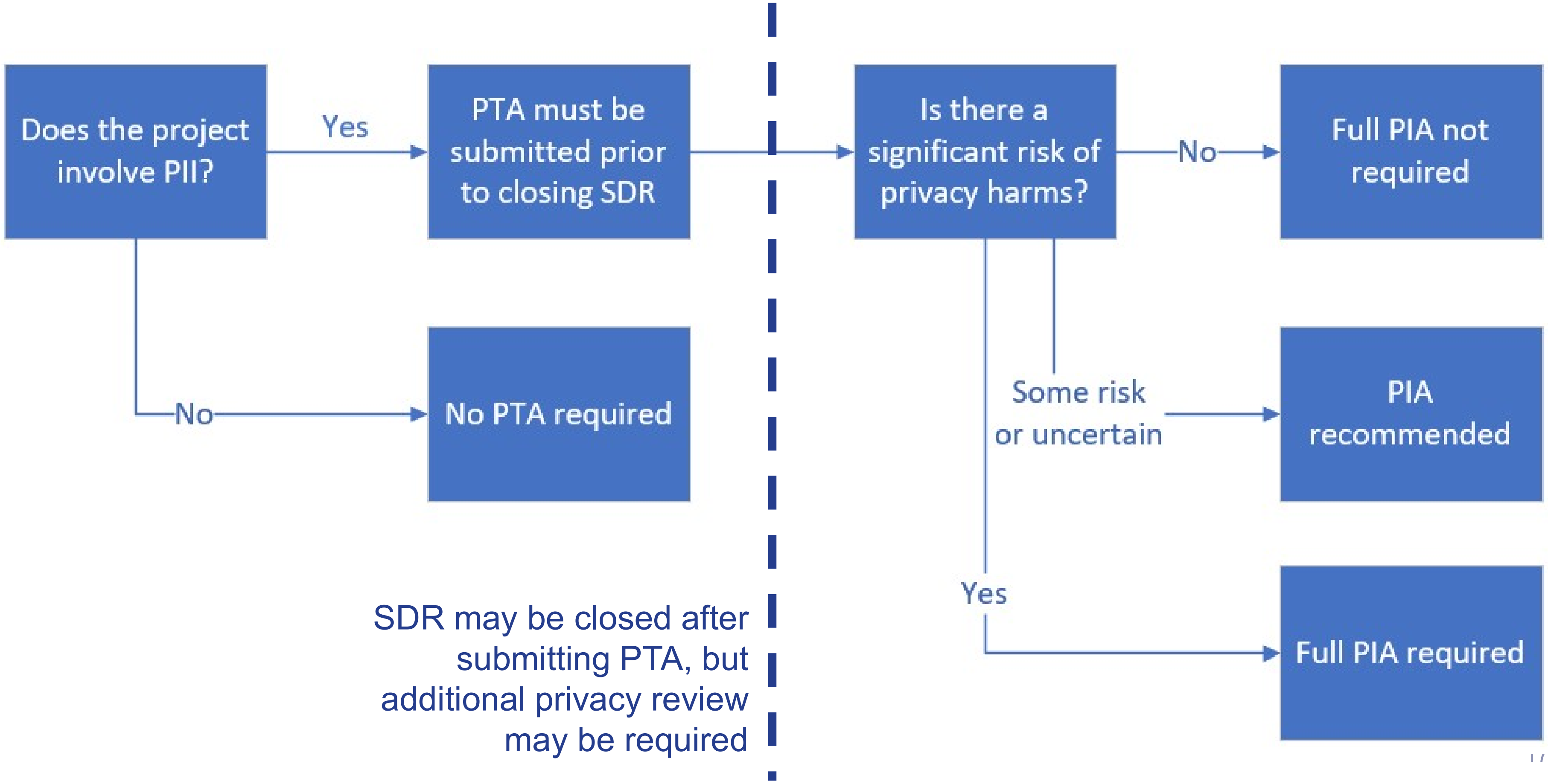
To WaTech mi OCIO Privacy;

DEMO-PRIVACY AUTO TEST-PTA.xlsx
34 KB

Hello! Thank you for completing the Security Design Review submission form. Based on your answers you have indicated that your project will be processing personally identifiable information (PII). As a part of the process to implement this technology, please complete the Privacy Threshold Analysis form. This will be referred to the Office of Privacy and Data Protection for review to determine potential privacy impacts. To submit the Privacy Threshold Analysis form, or if you have any questions, please email privacy@watech.wa.gov.
Thank you.

What if I don’t get an automated message?

- You will not receive an automated message if:
  - Outside of tenant
  - Answer submission form incorrectly
  - Understanding of project changes
- Send message to privacy@watech.wa.gov
- OPDP/OCS will monitor to identify projects that did not have PTA assigned



Does the project involve PII?

Yes

PTA must be submitted prior to closing SDR

No

No PTA required

Is there a significant risk of privacy harms?

No

Full PIA not required

Some risk or uncertain

PIA recommended

Yes

Full PIA required

SDR may be closed after submitting PTA, but additional privacy review may be required

WaTech
Washington Technology Solutions

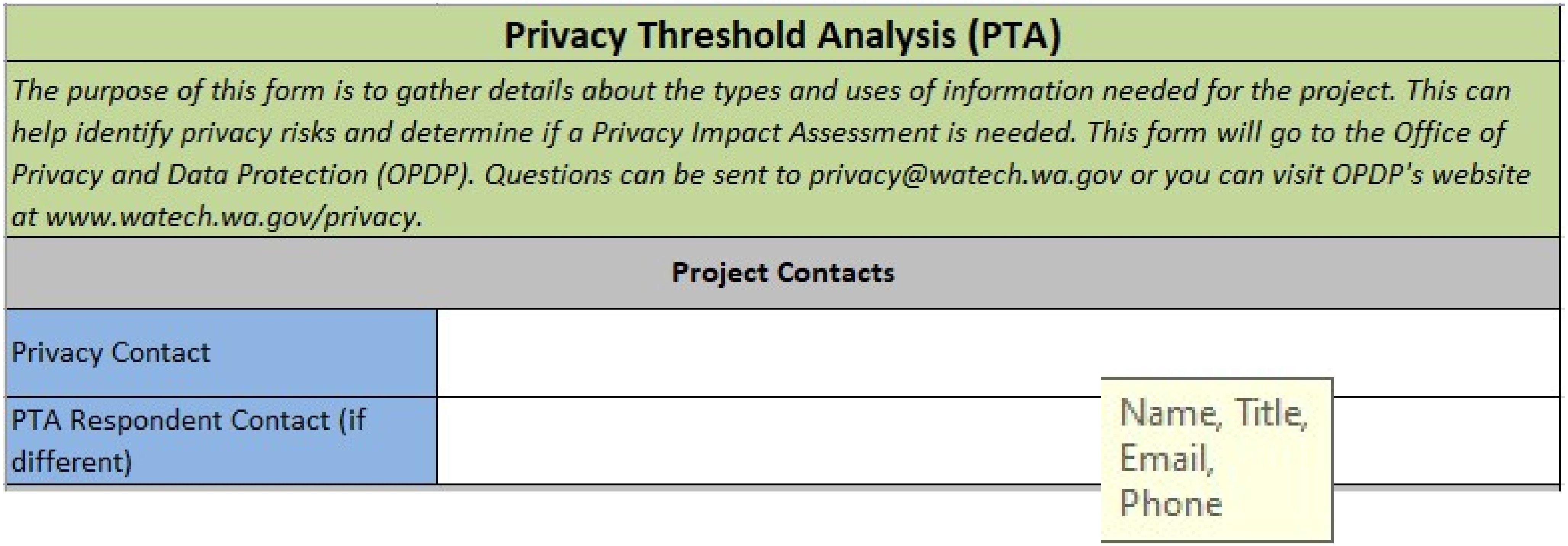
PTA completion tips

PTA Topics

- Privacy Contact (or person completing form)
- General description and purpose of project
- Is PII being collected, used, maintained, disclosed or otherwise processed?
- Information about which types of individuals will be included (e.g. public, minors, state employees)

- Highest level category of data?
- Does the project involve any of the following types of data?
  - (e.g. SSN, immigration/citizenship, financial or tax data, CJIS, biometric, health information, geolocation)
- Describe how data will be used and who may have access?
- External data sharing?

WaTech
Washington Technology Solutions



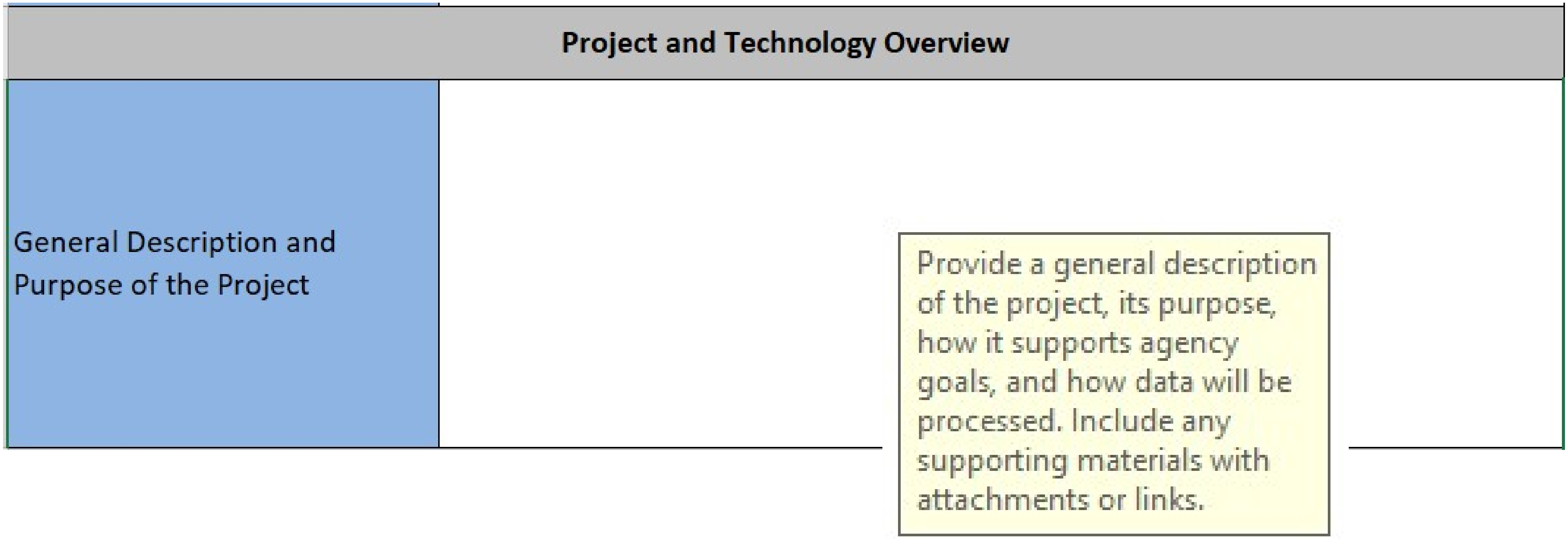
Privacy Threshold Analysis (PTA)

The purpose of this form is to gather details about the types and uses of information needed for the project. This can help identify privacy risks and determine if a Privacy Impact Assessment is needed. This form will go to the Office of Privacy and Data Protection (OPDP). Questions can be sent to privacy@watech.wa.gov or you can visit OPDP's website at www.watech.wa.gov/privacy.

Project Contacts

Privacy Contact	
PTA Respondent Contact (if different)	

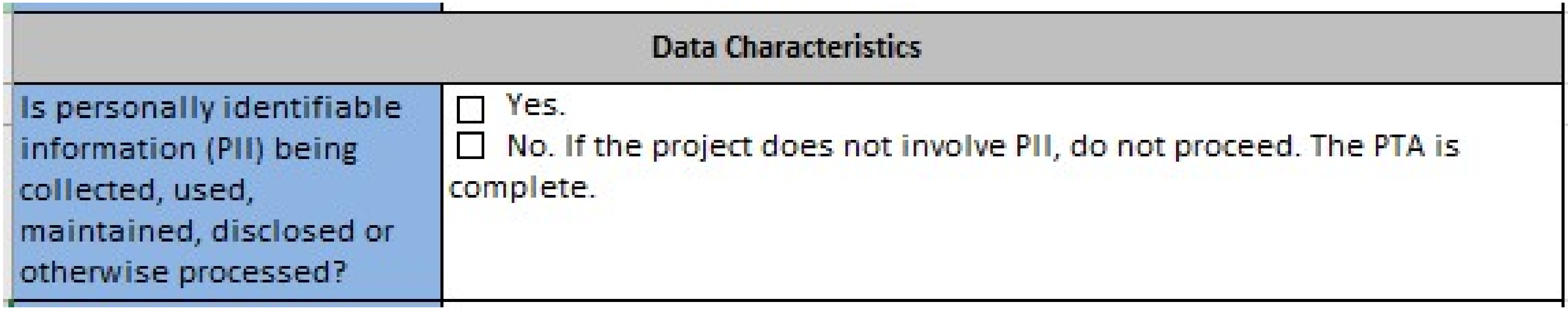
Name, Title, Email, Phone



Project and Technology Overview	
General Description and Purpose of the Project	

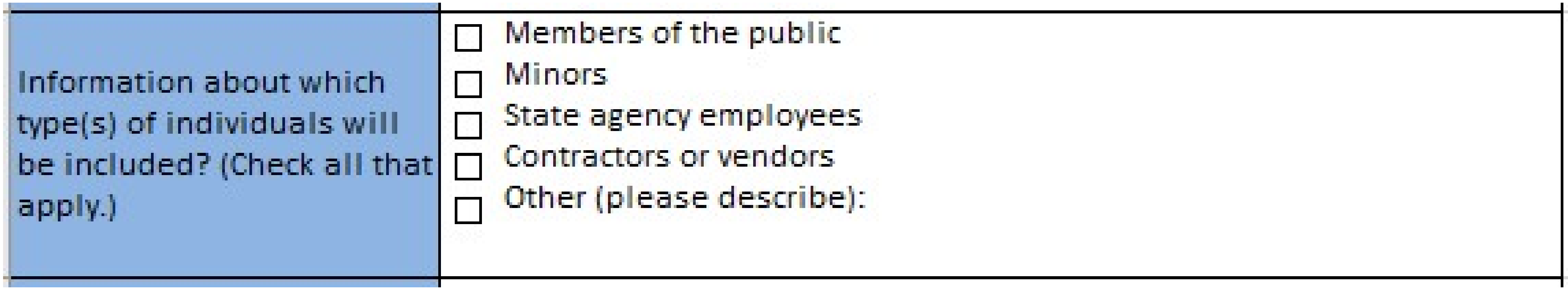
Provide a general description of the project, its purpose, how it supports agency goals, and how data will be processed. Include any supporting materials with attachments or links.

Data characteristics



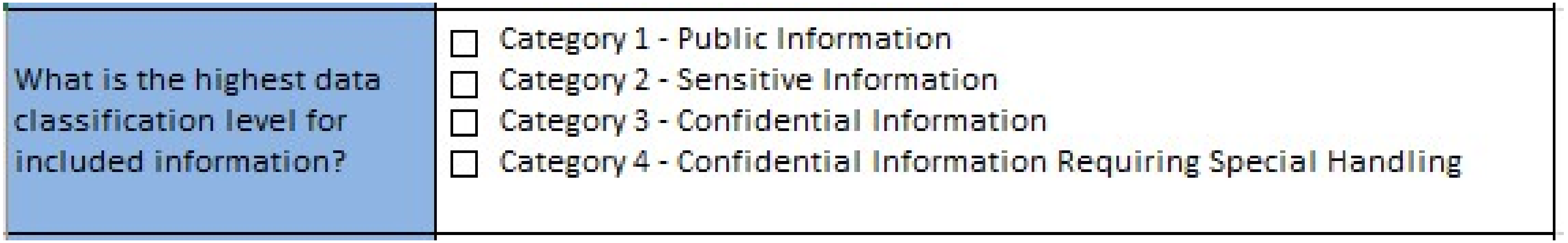
Data Characteristics	
Is personally identifiable information (PII) being collected, used, maintained, disclosed or otherwise processed?	□ Yes. □ No. If the project does not involve PII, do not proceed. The PTA is complete.

Data characteristics



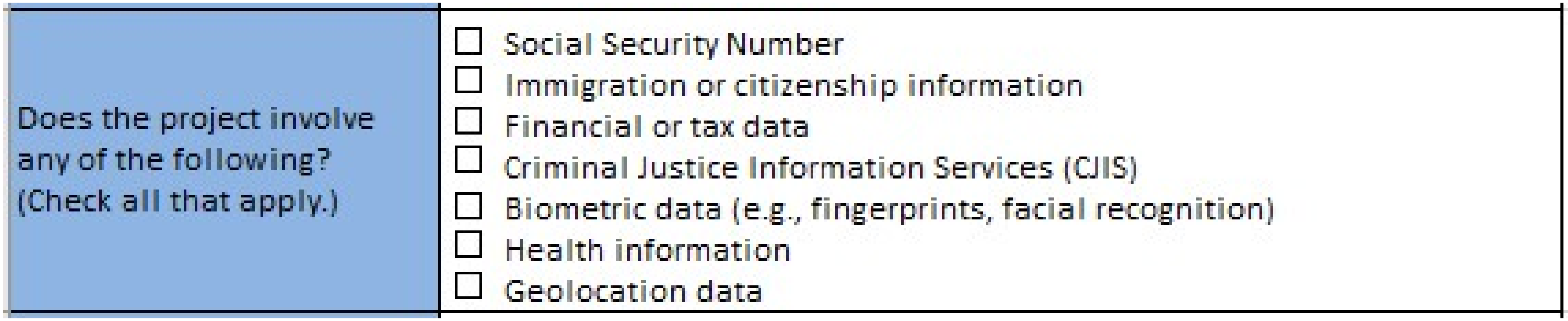
Information about which type(s) of individuals will be included? (Check all that apply.)	□ Members of the public □ Minors □ State agency employees □ Contractors or vendors □ Other (please describe):

Data characteristics



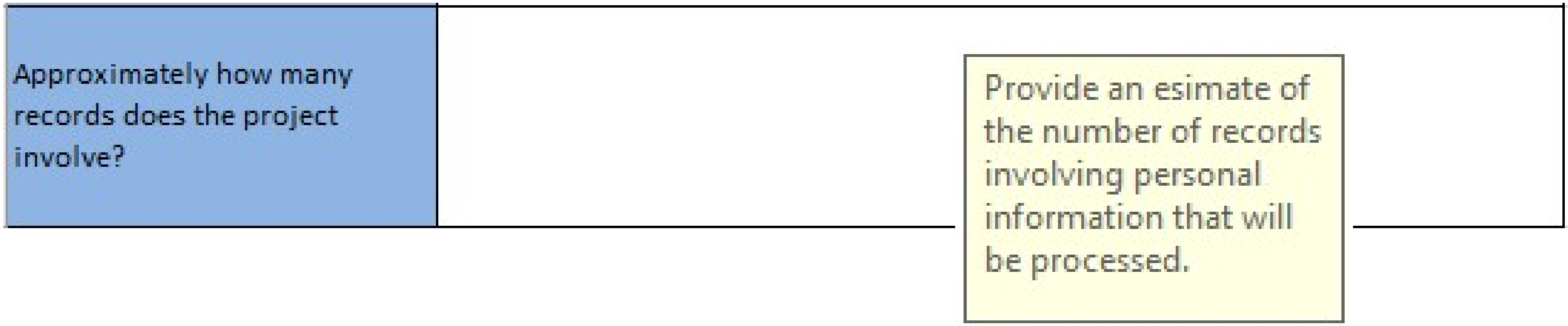
What is the highest data classification level for included information?	□ Category 1 - Public Information □ Category 2 - Sensitive Information □ Category 3 - Confidential Information □ Category 4 - Confidential Information Requiring Special Handling

Data characteristics



Does the project involve any of the following? (Check all that apply.)	□ Social Security Number □ Immigration or citizenship information □ Financial or tax data □ Criminal Justice Information Services (CJIS) □ Biometric data (e.g., fingerprints, facial recognition) □ Health information □ Geolocation data

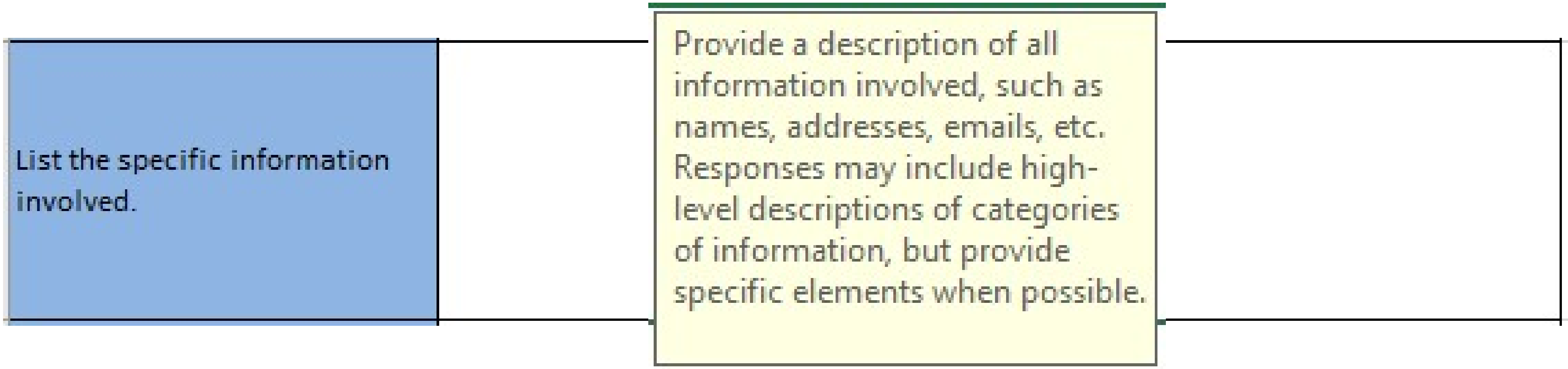
Data characteristics



Approximately how many records does the project involve?	

Provide an esimate of the number of records involving personal information that will be processed.

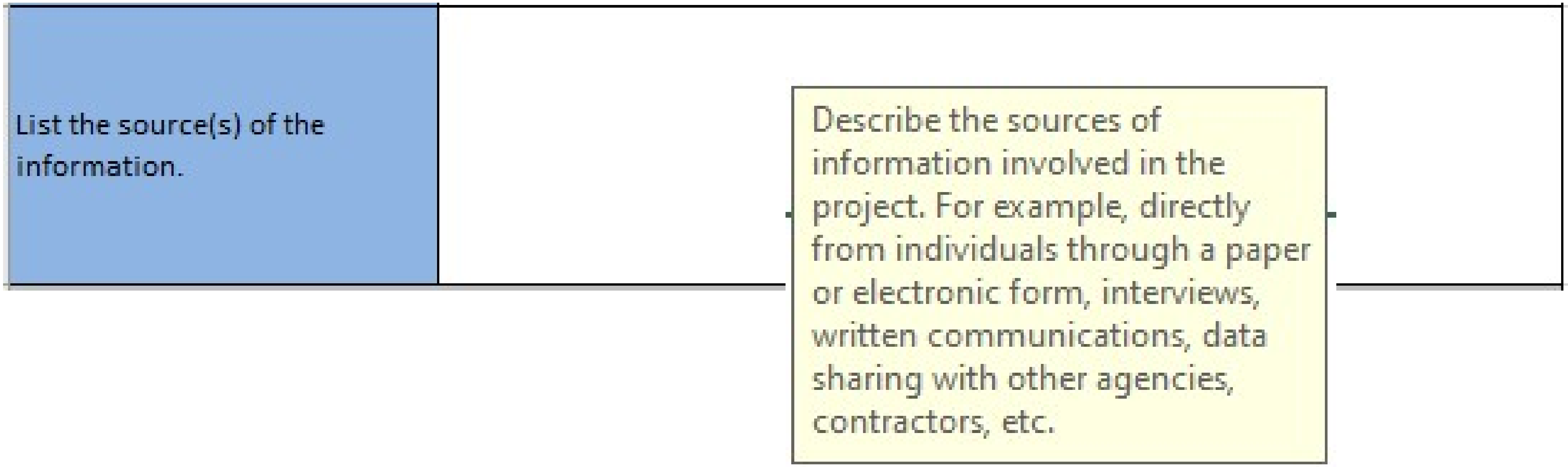
Data characteristics



List the specific information involved.

Provide a description of all information involved, such as names, addresses, emails, etc. Responses may include high-level descriptions of categories of information, but provide specific elements when possible.

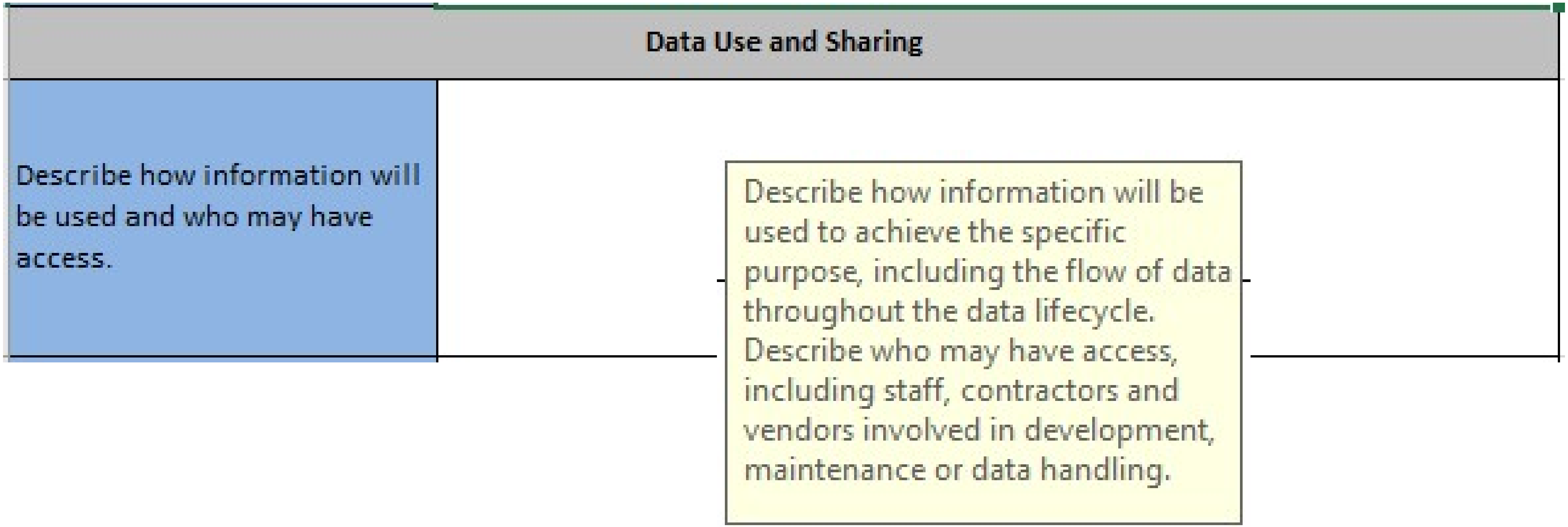
Data characteristics



List the source(s) of the information.	

Describe the sources of information involved in the project. For example, directly from individuals through a paper or electronic form, interviews, written communications, data sharing with other agencies, contractors, etc.

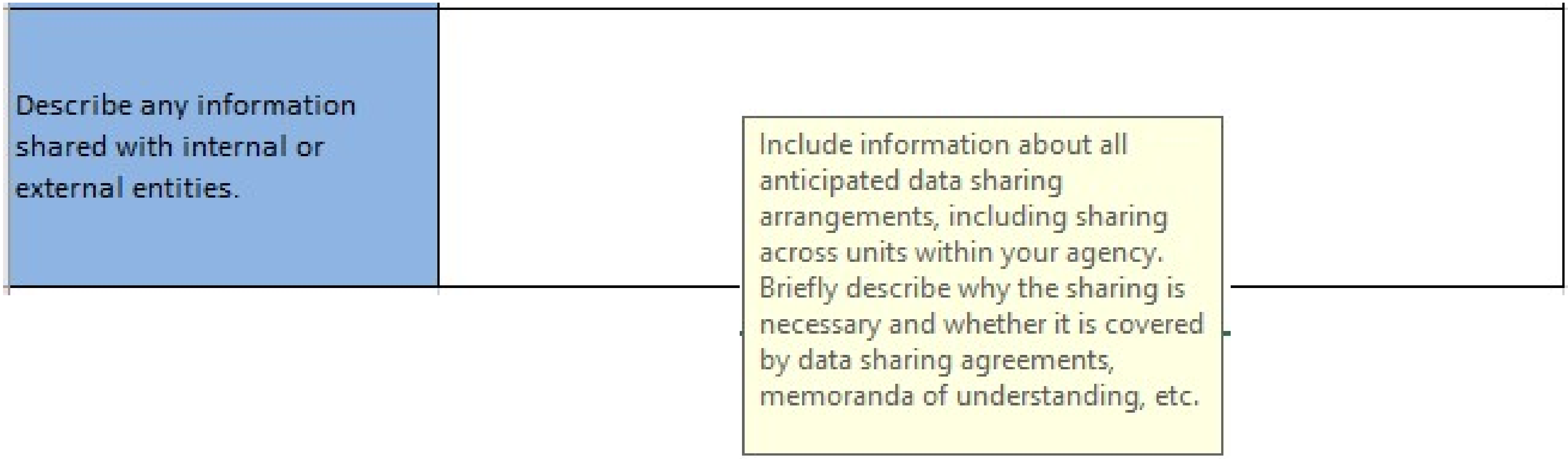
Data use and sharing



Data Use and Sharing	
Describe how information will be used and who may have access.	

Describe how information will be used to achieve the specific purpose, including the flow of data throughout the data lifecycle. Describe who may have access, including staff, contractors and vendors involved in development, maintenance or data handling.

Data use and sharing



Describe any information shared with internal or external entities.	

Include information about all anticipated data sharing arrangements, including sharing across units within your agency. Briefly describe why the sharing is necessary and whether it is covered by data sharing agreements, memoranda of understanding, etc.

WaTech
Washington Technology Solutions

Introduction to PIAs

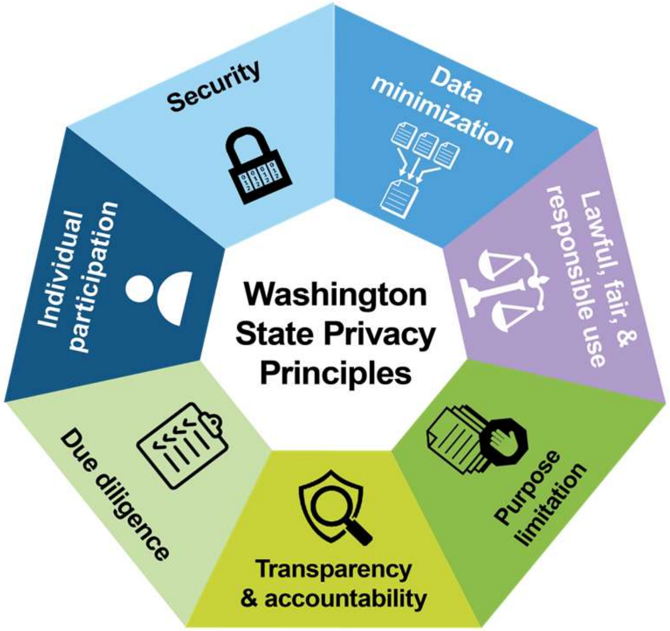
When is a PIA required?

- The Privacy Threshold Analysis (PTA) is a brief, high-level document that gathers the intended types and uses of personal information.
- It is used to help determine whether a Privacy Impact Assessment (PIA) should be conducted.
- A PIA should be conducted when there is a significant risk of privacy harms.
- What factors should be considered?

When is a PIA required?

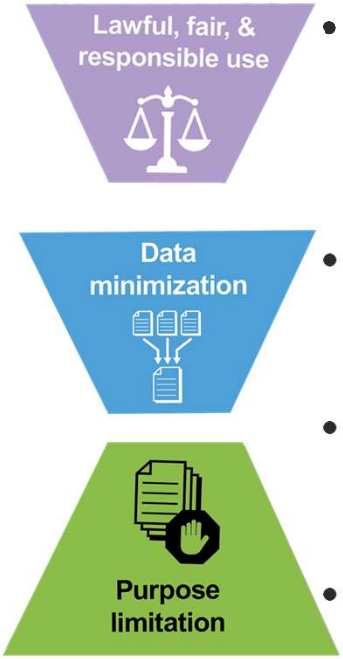
Factors that could indicate heightened risk	
Considerations for sensitive information	Considerations for processing activities
Race or ethnicity	Selling data
Religious or philosophical beliefs	Using new technologies
Mental or physical health	Monitoring geolocation
Sex life or sexual orientation	Large scale processing, including monitoring a public place on a large scale
Citizenship or immigration status	Using data to make automated decisions that could have legal or similarly significant effects
Genetic or biometric information	Profiling that could foreseeably lead to unfair or disparate impact on individuals
Information about minors	

PIA Analysis Aligns to Washington State Privacy Principles

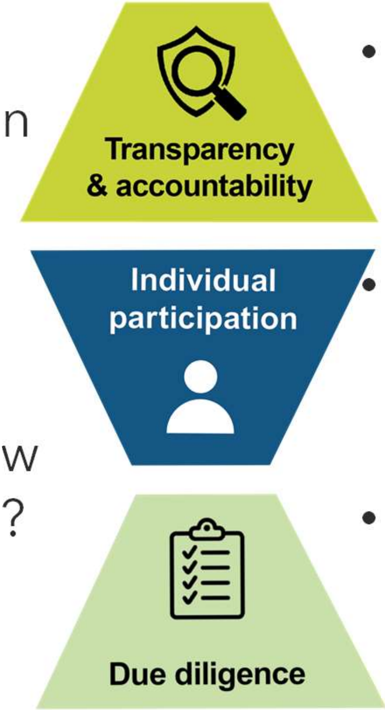

Washington State Privacy Principles
Security
Data minimization
Lawful, fair, & responsible use
Purpose limitation
Transparency & accountability
Due diligence
Individual participation

- Washington State Agency Privacy Principles
- Public agencies have an obligation to handle PII about Washington residents and employees in fair and transparent way to ensure public trust.

PIA Analysis Aligns to Washington State Privacy Principles



- What are the legal authorities for collection & use of PII?
- Sources of PII? Data elements needed?
- Purpose of project? How does it support agency?
- Who has access to PII



- Is notice provided? Who or why not? How is agency ensuring compliance?
- Opt in? Opt out? Decline? Access? Correct? Procedures?
- 3rd party access to PII? Agreements in place? Records of disclosures?

Benefits of PIA

- Helps agency be intentional about:
- Collection, Use, Sharing, Protecting PII
- Proactive adoption of policies and procedures for treatment of PII
- Mitigates harm and risk
- Public trust

PIA Process

- After review of PTA, you will receive an email stating whether or not the project requires a PIA.
- Rough numbers – out of approx. 35 PTAs 4 so far have required PIA. Involve your privacy professionals in PTA.
- OPDP is here to help! PIAs should not and do not need to be completed on your own. We are here to help think through answers and best way to complete PIA and mitigate risk. It should be a consultative process.

WaTech
Washington Technology Solutions

Questions?

Website

- watech.wa.gov/Privacy

Email

- privacy@watech.wa.gov