 Agenda

- Background
- The PIA Process
- PIA Example

This document is proprietary and confidential. No part of it may be disclosed, in any manner, without prior written consent of Kuma, LLC, or the intended recipient, State of Washington OCIO-OPDP.
Before We Get Started

• Privacy and the protection of personal information are at the core of government.
• Privacy Impact Assessments (PIA) are best practice.
• Privacy may look different at each state agency.
• The OPDP acts as a valuable resource for state agencies.

• Key terms and phrases
  o Personally Identifiable Information (PII)
  o Project
  o Risk
PIA as a Privacy Best Practice

- PIAs are found across all industries and are completed by organizations across the globe.

- PIAs can be completed in any format, including word documents and spreadsheets.

- PIAs are tools that serve multiple purposes, including government transparency.
Federal Policy and Guidance

• **E-Government Act of 2002**
  o Required federal agencies to conduct PIA, to have them reviewed by agency leadership, and to post them publicly

  o Provided clarification on requirements, identified common PIA triggers, exceptions, and PIA content, depth, and breadth

• **OMB M-16-24 – Role and Designation of Senior Agency Officials for Privacy**
  o Elevated the role of SAOP and added responsibilities related to privacy compliance efforts, privacy risk management

• **OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information**
  o Establishes the PIA as a tool to assist in data breach response
OMB M-03-22, Section II. Privacy Impact Assessment

• When to Conduct a PIA (“PIA Triggers”)
  - Conversions
  - Anonymous to Non-Anonymous
  - Significant System Management Changes
  - Significant Merging
  - New Public Access
  - Commercial Sources
  - New Interagency Uses
  - Internal Flow or Collection
  - Alteration in Character of Data

• Conducting a PIA – Content
  - What information is collected
  - Why information is collected
  - Intended use of information
  - With whom information is shared
  - Opportunities for individuals to decline to provide information and how individuals can grant consent
  - How information will be secured
  - Analysis: choices made by the agency regarding the system, as a result of the PIA (mitigation)

• Publishing a PIA
The PIA Process
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.

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.

Continuous Review Cycle

Privacy Impact Assessment (PIA)

Review and Update, as Appropriate
The PIA Process

• **Preparation**
  - Ensure a clear understanding of the process, roles, and responsibilities.
  - Define the scope of the review.

• **PTA**
  - Provide a high-level overview 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.
PIA Example

DHS/TSA/PIA-032
Advanced Imaging Technology (AIT)

- DHS/TSA/PIA-032 - Advanced Imaging Technology (AIT) – 2008
- DHS/TSA/PIA-032-a - Advanced Imaging Technology (AIT) – 2009
- DHS/TSA/PIA-032-b - Advanced Imaging Technology (AIT) – 2008
- DHS/TSA/PIA-032-c - Advanced Imaging Technology (AIT) – 2011
- DHS/TSA/PIA-032-d - Advanced Imaging Technology (AIT) – 2015

“TSA Body Scanners”

This document is proprietary and confidential. No part of it may be disclosed, in any manner, without prior written consent of Kuma, LLC, or the intended recipient, State of Washington OCIO-OPDP.
OMB M-03-22, Section II. Privacy Impact Assessment

• When to Conduct a PIA (“PIA Triggers”)
  o Conversions
  o Anonymous to Non-Anonymous
  o Significant System Management Changes
  o Significant Merging
  o New Public Access
  o Commercial Sources
  o New Interagency Uses
  o Internal Flow or Collection
  o Alteration in Character of Data

• Conducting a PIA – Content
  o What information is collected
  o Why information is collected
  o Intended use of information
  o With whom information is shared
  o Opportunities for individuals to decline to provide information and how individuals can grant consent
  o How information will be secured
  o Analysis: choices made by the agency regarding the system, as a result of the PIA (mitigation)

• Publishing a PIA
DHS PIA Contents

• Abstract
• Introduction
• Analysis using the Fair Information Practice Principles (FIPPs)
  o Transparency
  o Individual Participation
  o Purpose Specification
  o Data Minimization
  o Use Limitation
  o Data Quality and Integrity
  o Security
  o Accountability
• Conclusion
The PIA Process

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) → Review and Update, as Appropriate

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.
Thank you!

Contact for Questions:
Ivy.Orecchio@kuma.pro