



**State of Washington,  
Office of Privacy and Data Protection (OPDP)**

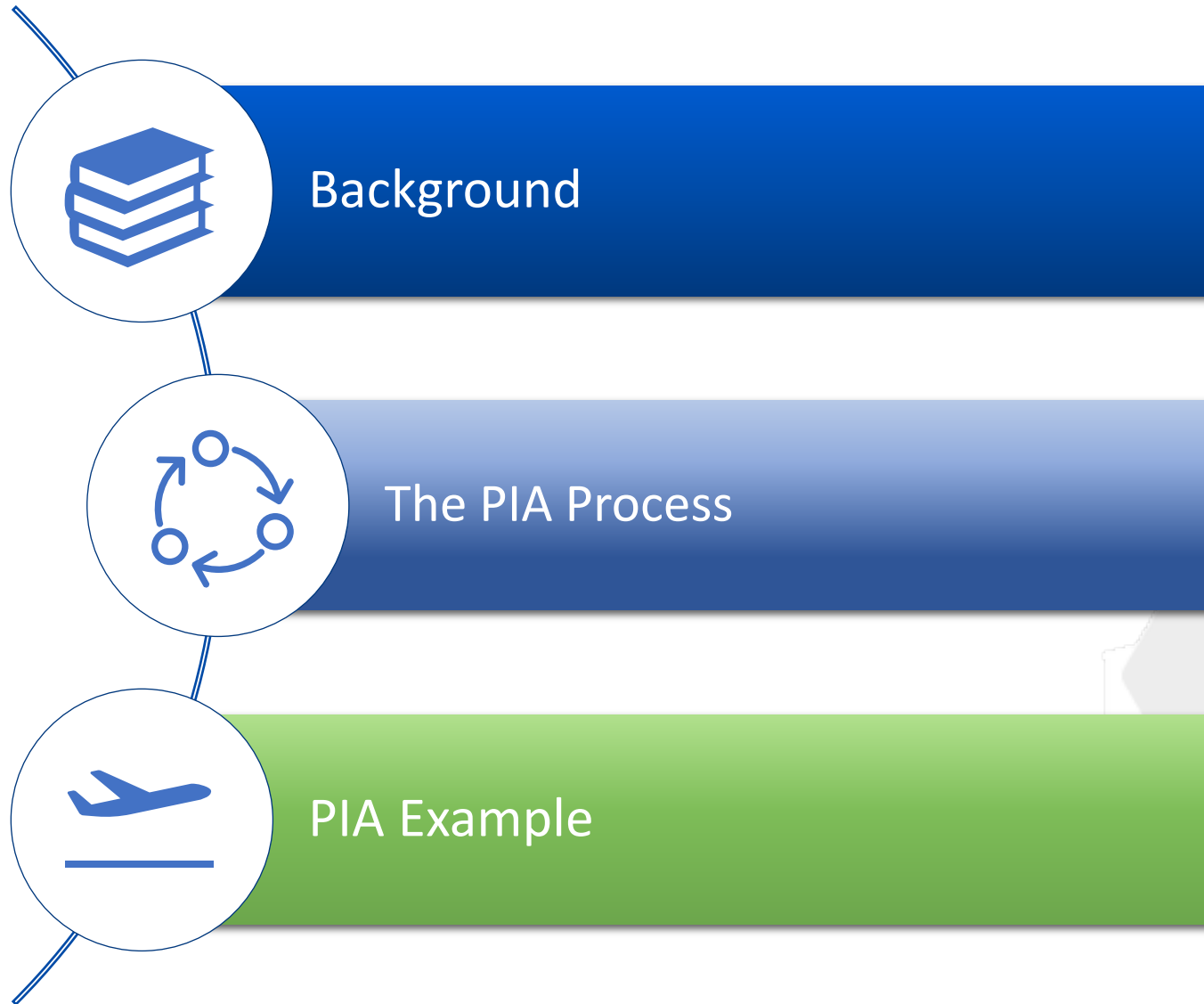
# **Privacy Impact Assessments**

**October 21, 2021**

**Presented by:  
Ivy Orecchio, Director of Privacy**



# Agenda



# Before We Get Started

- Privacy and the protection of personal information are at the core of government.
- Privacy Impact Assessments (PIAs) are the best practice.
- Privacy may look different in different agencies.
- The OPDP acts as a voice for the agencies.
- Key terms and phrases
  - Personally Identifiable Information
  - Project
  - 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**

- Required federal agencies to conduct PIA, to have them reviewed by agency leadership, and to post them publicly

- **OMB M-03-22 - OMB Guidance for Implementing the Privacy Provisions of the E- Government Act of 2002**

- 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**

- 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**

- 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**


M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 8/16/19, 3:46 PM

This is historical material, "frozen in time" and not current OMB guidance. The web site is no longer updated and links to external web sites and some internal pages will not work.

 OFFICE OF MANAGEMENT AND BUDGET

September 26, 2003

M-03-22  
MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Joshua B. Bolton  
Director 

SUBJECT: OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002

The attached guidance provides information to agencies on implementing the privacy provisions of the E-Government Act of 2002, which was signed by the President on December 17, 2002 and became effective on April 17, 2003.

The Administration is committed to protecting the privacy of the American people. This guidance document addresses privacy protections when Americans interact with their government. The guidance directs agencies to conduct reviews of how information about individuals is handled within their agency when they use information technology (IT) to collect new information, or when agencies develop or buy new IT systems to handle collections of personally identifiable information. Agencies are also directed to describe how the government handles information that individuals provide electronically, so that the American public has assurances that personal information is protected.

The privacy objective of the E-Government Act complements the National Strategy to Secure Cyberspace. As the National Strategy indicates, cyberspace security programs that strengthen protections for privacy and other civil liberties, together with strong privacy policies and practices in the federal agencies, will ensure that information is handled in a manner that maximizes both privacy and security.

**Background**

Section 208 of the E-Government Act of 2002 (Public Law 107-347, 44 U.S.C. Ch 36) requires that OMB issue guidance to agencies on implementing the privacy provisions of the E-Government Act (see Attachment A). The text of section 208 is provided as Attachment B to this Memorandum. Attachment C provides a general outline of regulatory requirements pursuant to the Children's Online Privacy Protection Act ("COPPA"). Attachment D summarizes the modifications to existing guidance resulting from this Memorandum. A complete list of OMB privacy guidance currently in effect is available at OMB's website.

As OMB has previously communicated to agencies, for purposes of their FY2005 IT budget requests, agencies should submit all required Privacy Impact Assessments no later than October 3, 2003.

For any questions about this guidance, contact Eva Kleederman, Policy Analyst, Information Policy and Technology Branch, Office of Management and Budget, phone (202) 395-3647, fax (202) 395-5167, e-mail [Eva\\_Kleederman@omb.eop.gov](mailto:Eva_Kleederman@omb.eop.gov).

Attachments

- Attachment A
- Attachment B
- Attachment C
- Attachment D

Attachment A  
E-Government Act Section 208 Implementation Guidance

<https://georgewbush-whitehouse.archives.gov/omb/memoranda/m03-22.html> Page 1 of 13

# The PIA Process

# 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)

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



# The PIA Process

- **Preparation**

- Ensure a clear understanding of the project and the 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**

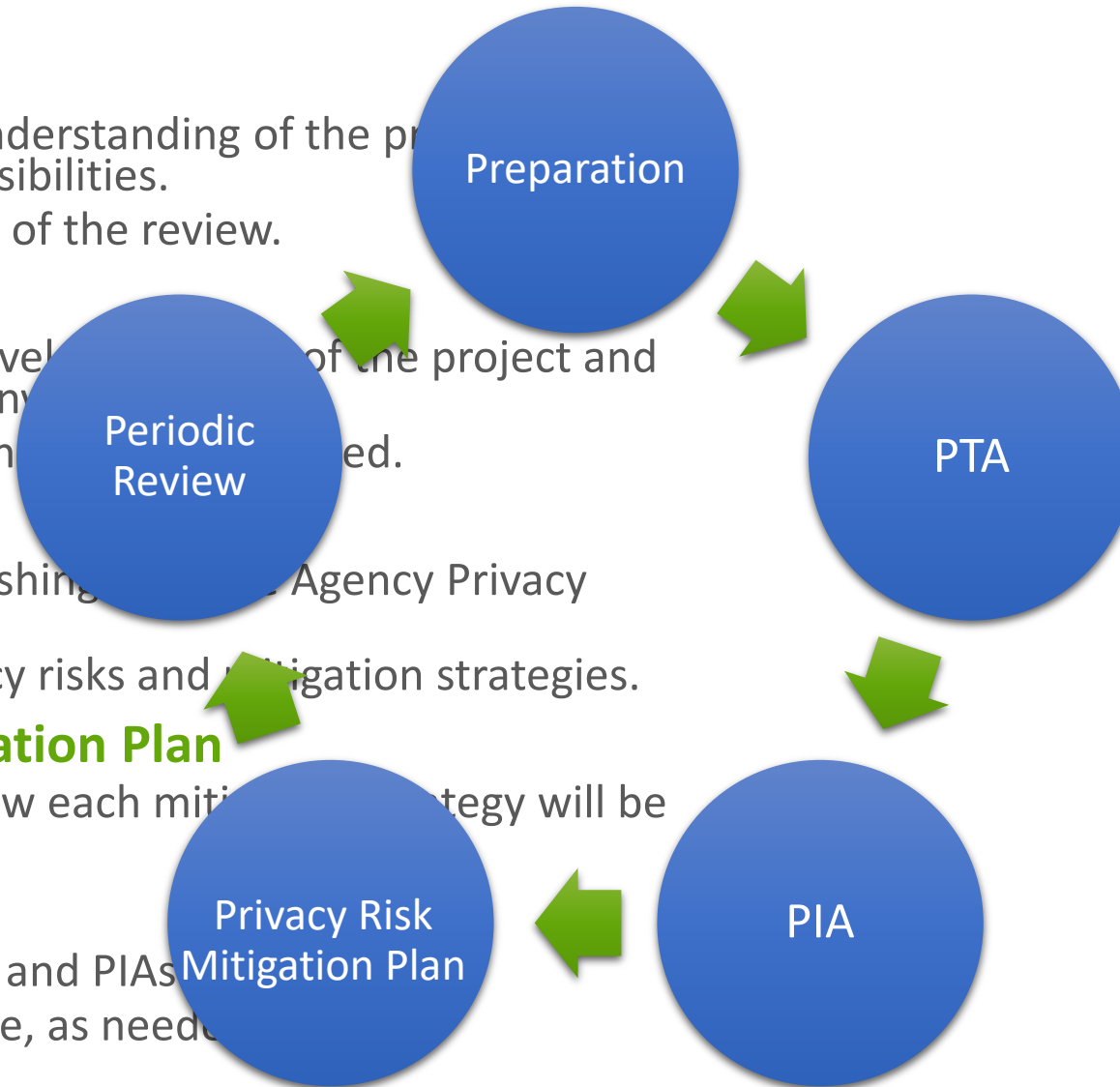
- Consider the Washington State Agency Privacy Principles.
- Document privacy risks and mitigation strategies.

- **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”)**

- 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**

M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 8/16/19, 3:46 PM

This is historical material, "frozen in time" and not current OMB guidance. The web site is no longer updated and links to external web sites and some internal pages will not work.



OFFICE OF  
MANAGEMENT AND BUDGET

September 26, 2003

M-03-22  
MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Joshua B. Bolton  
Director

SUBJECT: OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002

The attached guidance provides information to agencies on implementing the privacy provisions of the E-Government Act of 2002, which was signed by the President on December 17, 2002 and became effective on April 17, 2003.

The Administration is committed to protecting the privacy of the American people. This guidance document addresses privacy protections when Americans interact with their government. The guidance directs agencies to conduct reviews of how information about individuals is handled within their agency when they use information technology (IT) to collect new information, or when agencies develop or buy new IT systems to handle collections of personally identifiable information. Agencies are also directed to describe how the government handles information that individuals provide electronically, so that the American public has assurances that personal information is protected.

The privacy objective of the E-Government Act complements the National Strategy to Secure Cyberspace. As the National Strategy indicates, cyberspace security programs that strengthen protections for privacy and other civil liberties, together with strong privacy policies and practices in the federal agencies, will ensure that information is handled in a manner that maximizes both privacy and security.

**Background**

Section 208 of the E-Government Act of 2002 (Public Law 107-347, 44 U.S.C. Ch 36) requires that OMB issue guidance to agencies on implementing the privacy provisions of the E-Government Act (see Attachment A). The text of section 208 is provided as Attachment B to this Memorandum. Attachment C provides a general outline of regulatory requirements pursuant to the Children's Online Privacy Protection Act ("COPPA"). Attachment D summarizes the modifications to existing guidance resulting from this Memorandum. A complete list of OMB privacy guidance currently in effect is available at OMB's website.

As OMB has previously communicated to agencies, for purposes of their FY2005 IT budget requests, agencies should submit all required Privacy Impact Assessments no later than October 3, 2003.

For any questions about this guidance, contact Eva Kleederman, Policy Analyst, Information Policy and Technology Branch, Office of Management and Budget, phone (202) 395-3647, fax (202) 395-5167, e-mail [Eva\\_Kleederman@omb.eop.gov](mailto:Eva_Kleederman@omb.eop.gov).

Attachments

- Attachment A
- Attachment B
- Attachment C
- Attachment D

Attachment A  
E-Government Act Section 208 Implementation Guidance

<https://georgewbush-whitehouse.archives.gov/omb/memoranda/m03-22.html> Page 1 of 13

# DHS PIA Contents

- **Abstract**
- **Introduction**
- **Analysis using the Fair Information Practice Principles (FIPPs)**
  - Transparency
  - Individual Participation
  - Purpose Specification
  - Data Minimization
  - Use Limitation
  - Data Quality and Integrity
  - Security
  - Accountability
- **Conclusion**



Privacy Impact Assessment  
for  
**TSA Whole Body Imaging**

**January 2, 2008**

**Contact Point**

**Mike Golden**  
Assistant Administrator  
Operational Process & Technology  
Mike.Golden@dhs.gov

**Reviewing Official**

**Peter Pietra**  
Director, Privacy Policy & Compliance  
Transportation Security Administration  
TSAprivacy@dhs.gov

**Hugo Teufel III**  
Chief Privacy Officer  
Department of Homeland Security  
Privacy@dhs.gov

# 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)

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

# Thank you!

Contact for Questions:

Ivy.Orecchio@kuma.pro

