# Operationalizing Privacy

## Compliance Frameworks & Privacy Impact Assessments

Homeland Security

The Privacy Office

U.S. Department of Homeland Security
Washington, DC 20528
t: 571-227-3813; f: 571-227-4171
privacy@dhs.gov; www.dhs.gov/privacy

# Maureen Cooney

Acting Chief Privacy Officer

Chief Freedom of Information Act Officer

U.S. Department of Homeland Security

# Kip Hawley

## Assistant Secretary for Homeland Security and Director

## Transportation Security Administration

## U.S. Department of Homeland Security

Homeland Security

# Panel I: Operationalizing Privacy

## Moderator: Toby Milgrom Levin
### Senior Advisor, DHS Privacy Office

- Jane Horvath, Department of Justice
- Zoe Strickland, United States Postal Service
- Harriet P. Pearson, IBM Corporation
- Maya A. Bernstein, Health & Human Services

Homeland Security

# Panel II: Compliance

## Federal Requirements: SORNs, PIAs, C&A, OMB-300

Moderator: Hugo Teufel,
DHS Associate General Counsel for General Law

- Eva Kleederman, Office of Management & Budget
- Elizabeth Withnell, Chief Counsel, Privacy Office
- Bob West, DHS Chief Information Security Officer
- Barbara Symonds, Internal Revenue Service

Homeland Security

# Privacy Impact Assessment Training


Rebecca J. Richards

Director of Privacy Compliance

Nathan B. Coleman

PIA Coordinator

The Privacy Office

U.S. Department of Homeland Security

Washington, DC 20528

(571) 227-3813

pia@dhs.gov


Homeland Security

# Agenda

- Privacy Documentation
- When is a Privacy Impact Assessment (PIA) required?
- The Content of a PIA
- The PIA review process

# Privacy Documentation

- Updated Privacy Threshold Analysis
- Privacy Impact Assessment
- System of Records Notice

# Privacy Documentation

Updated
Privacy Threshold
Analysis

Homeland
Security

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
571-227-3813, pia@dhs.gov
www.dhs.gov/privacy



**PRIVACY THRESHOLD ANALYSIS**

Please complete this form and send it to the DHS Privacy Office.
Upon receipt, the DHS Privacy Office will review this form
and may request additional information.

**SUMMARY INFORMATION**

**DATE submitted for review:**

**NAME of Project: <Please enter the project name here.>**

**TYPE of Project:**

☐ **Information Technology and/or System**

The E-Government Act of 2002 defines these terms by reference to the definition sections of Titles 40 and 44 of the United States Code. The following is a summary of those definitions:

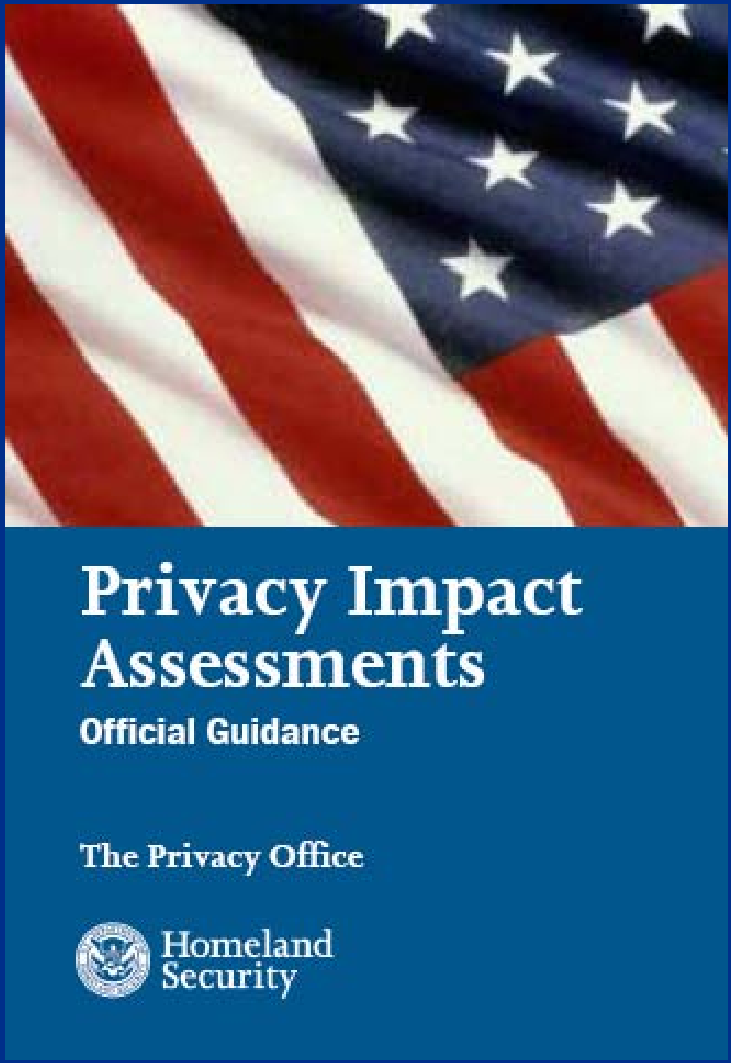
- "Information Technology" means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. See 40 U.S.C. § 11101(6).
- "Information System" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

Note, for purposes of this form, there is no distinction made between National Security Systems or technologies/systems managed by contractors. All technologies/systems should be initially reviewed for potential privacy impact.

☐ **A Notice of Proposed Rule Making or a Final Rule.**

# Privacy Documentation

Privacy Impact Assessment



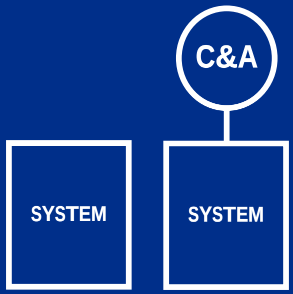

Homeland Security

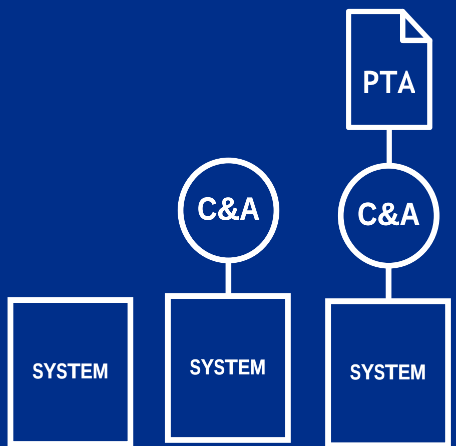
# Privacy Documentation

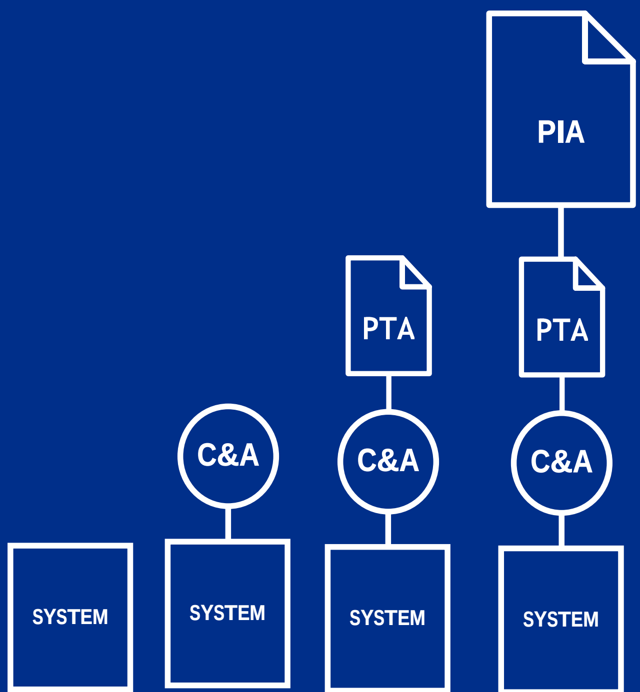
## System of Records Notice

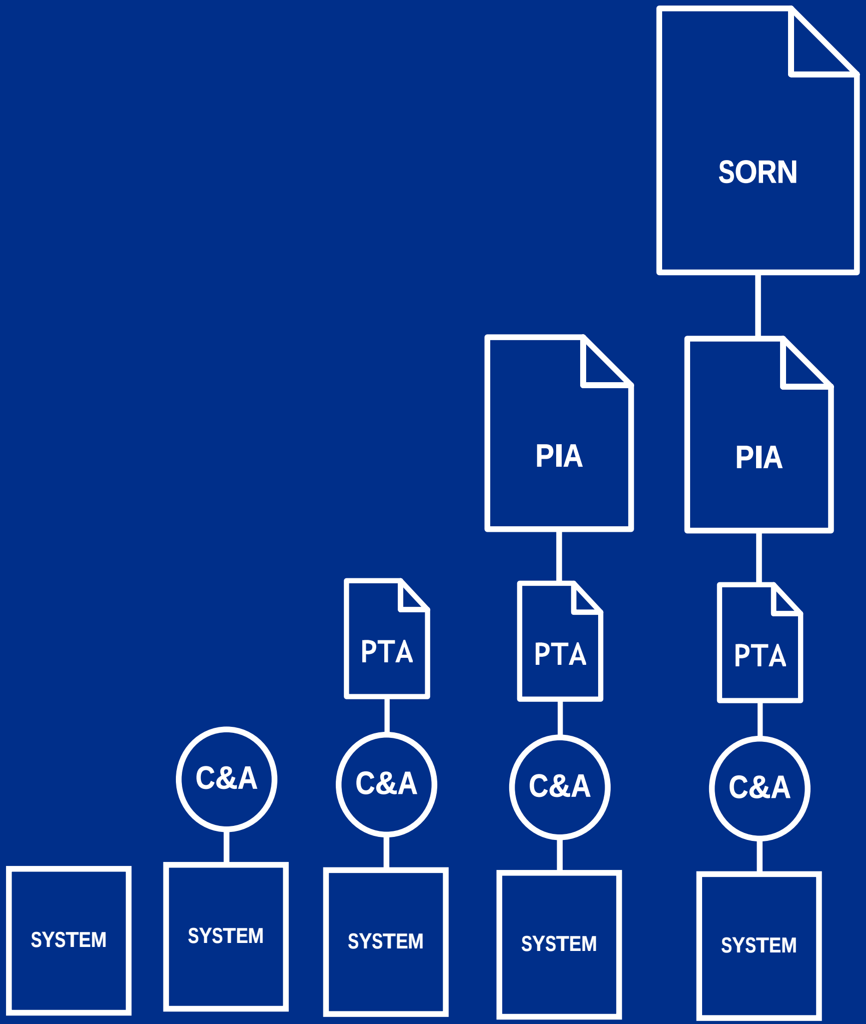
# How do these documents relate?

SYSTEM

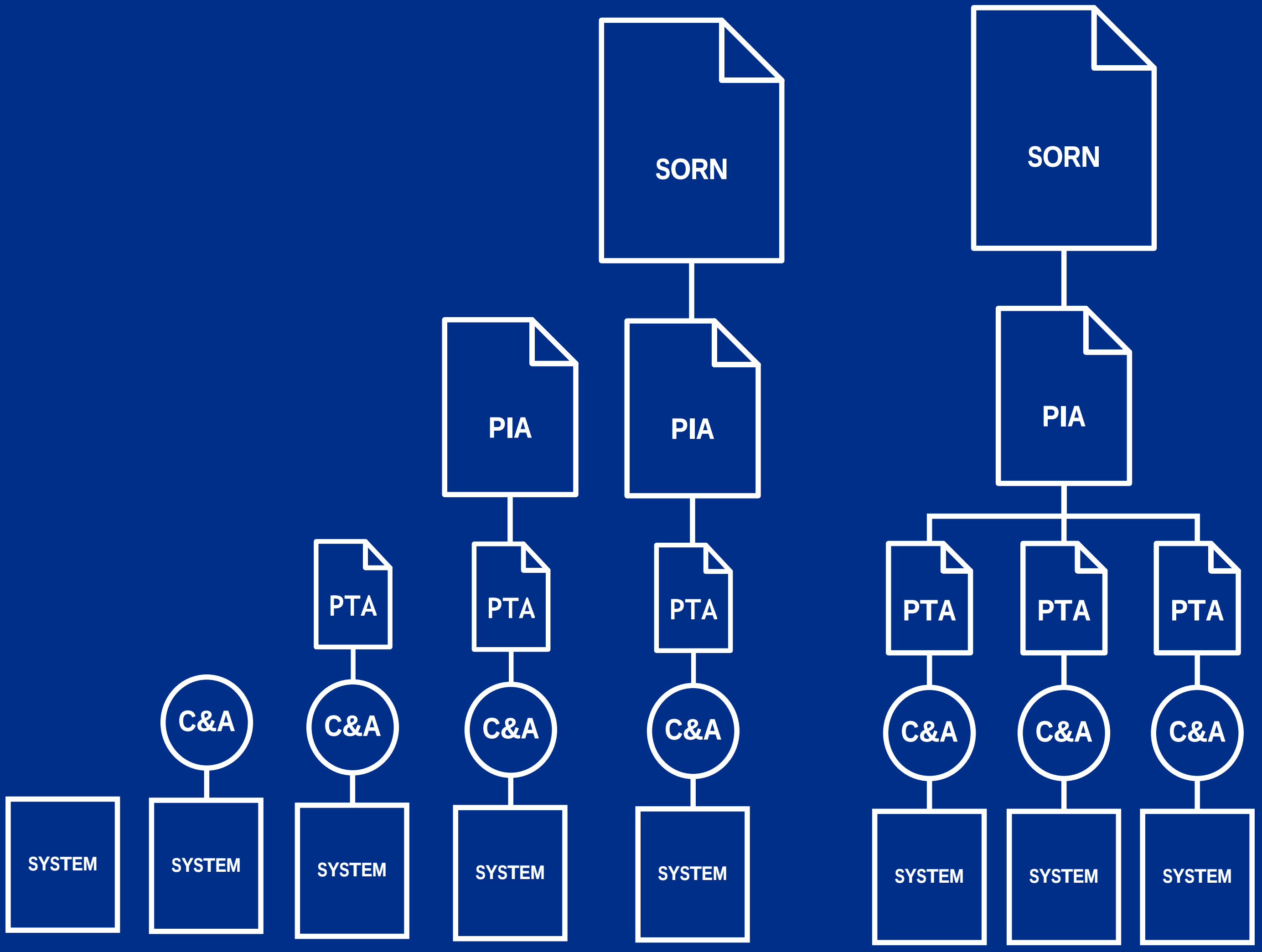

C&A
SYSTEM
SYSTEM


PTA
C&A
C&A
SYSTEM
SYSTEM
SYSTEM

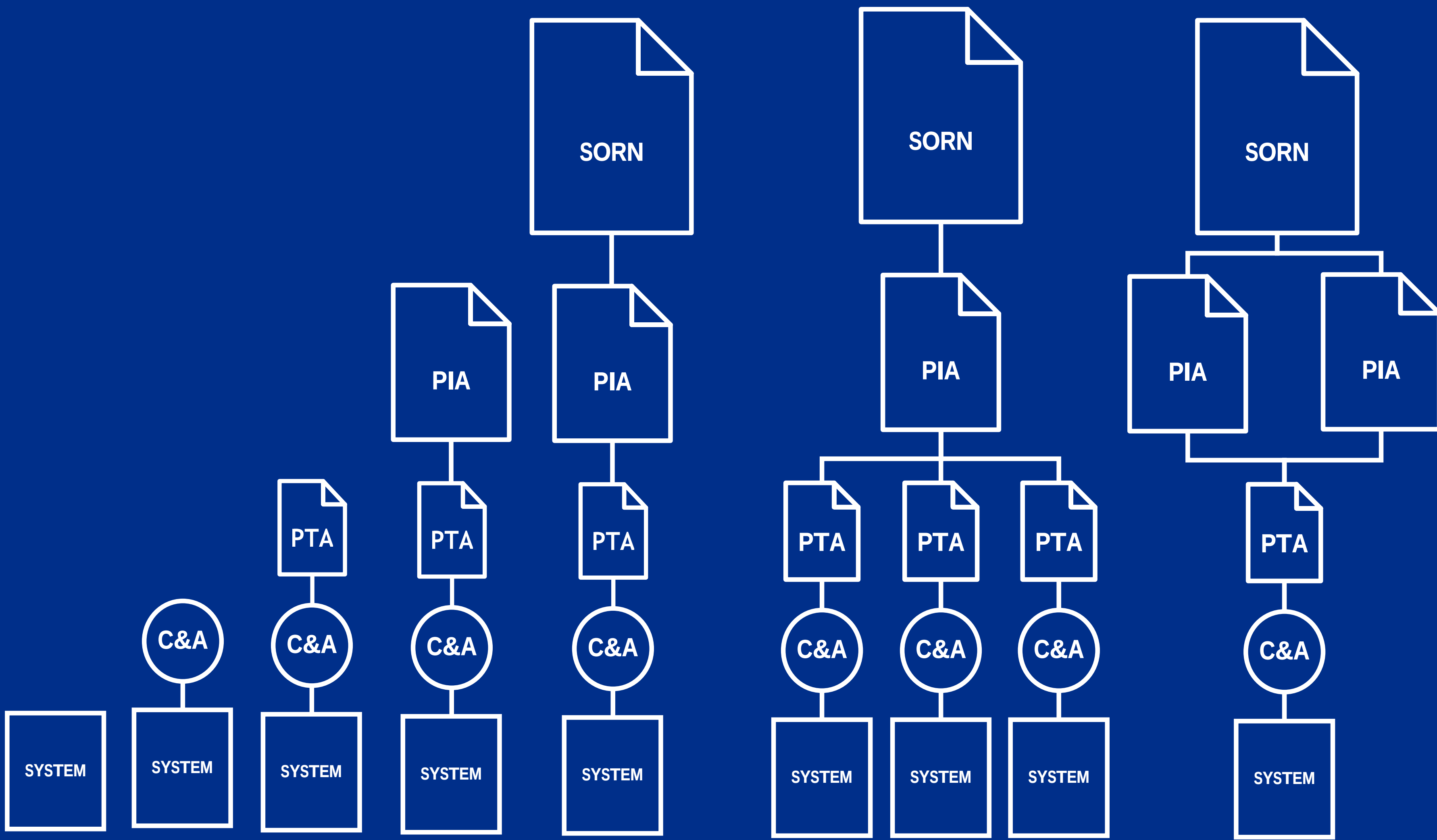

PIA
PTA
PTA
C&A
C&A
C&A
SYSTEM
SYSTEM
SYSTEM
SYSTEM



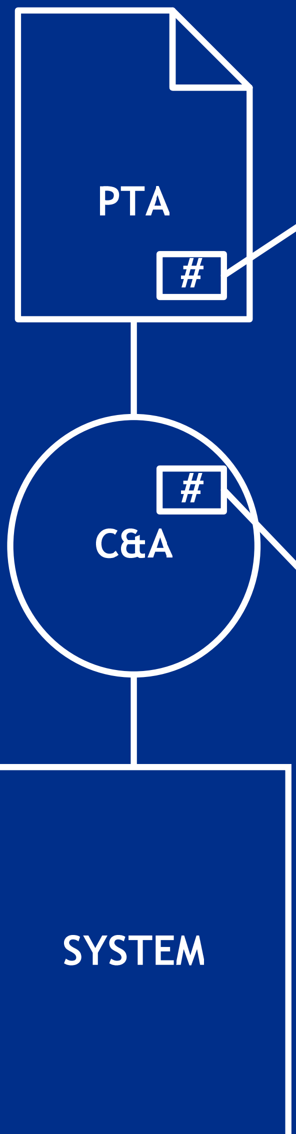

Homeland Security




Homeland Security




Homeland Security




<u>FIPS 199</u>
Confidentiality: [Low, Moderate, High, Undefined]
Integrity: [Low, Moderate, High, Undefined]
Availability: [Low, Moderate, High, Undefined]

<u>Personally Identifying Information</u>
Yes
HR
Legacy
National Security
No

<u>Status</u>
Privacy Impact Assessment:
[Not Applicable, Not Started, In Progress, Completed]

System of Records Notice:
[Not Applicable, Not Started, In Progress, Completed]

# TA FISMA

**Privacy**

**Privacy Threshold Assessment**

| | |
|---|---|
| PTA status: | Completed |
| Personally Identifiable Information: | Yes |
| PTA Date: | 05/11/2006 |

| New | | Support Document | Uploaded Date | Validated |
|---|---|---|---|---|
| Upload | Delete | Privacy Threshold Assessment | 06/08/2006 | Not Started |

**Privacy Impact Assessment**

| | |
|---|---|
| PIA status: | Completed |
| PIA Last Date: | 12/01/2005 |

| New | | Support Document | Uploaded Date | Validated |
|---|---|---|---|---|
| Upload | Delete | PIA Artifact | 12/11/2005 | ✓ |

**System of Records Notice**

| | |
|---|---|
| SORN status: | Completed |
| SORN Published Date: | 02/01/2006 |
| SORN ID: | 11.22.33.44.55 |

| New | | Support Document | Uploaded Date | Validated |
|---|---|---|---|---|
| Upload | Delete | System of Records Notice | 05/23/2006 | In Progress |

Homeland Security

# Privacy Documentation Requests

- OMB

# Privacy Documentation Requests

- OMB
- CIO’s Office and CFO’s Office

Homeland Security

# Privacy Documentation Requests

- OMB
- CIO's Office and CFO's Office
- General Counsel's Office

# Privacy Documentation Requests

- OMB
- CIO's Office and CFO's Office
- General Counsel's Office
- Inspector General's Office

# Privacy Documentation Requests

- OMB
- CIO's Office and CFO's Office
- General Counsel's Office
- Inspector General's Office
- General Accountability Office

# Risks of incomplete privacy documents

Homeland Security

# When is a PIA required?

- Developing or procuring any new technologies or systems that handle or collect personal information.
- Budget submissions to OMB that affect personal information.
- Pilot tests that affect personal information.
- Developing system revisions that affect personal information.
- Issuing a new or updated rulemaking that involves the collection, use, and maintenance of personal information.

Homeland Security

# How do you define:

- Personally Identifiable Information?
- Individual?

# When is a PIA NOT required?

- No changes since 2002?

# Writing the PIA

## Hypothetical

Homeland Security

The Privacy Office

U.S. Department of Homeland Security
Washington, DC 20528
t: 571-227-3813; f: 571-227-4171
privacy@dhs.gov; www.dhs.gov/privacy

# Specific Areas to Review

- Grandmother test
- No Trick Questions
- Use the template

# Introduction and Overview

- Context for the entire PIA
- Hypothetical

Homeland Security

# Section 1.0

- Information Collected and Maintained

# Section 1.0 Info. Collected & Maintained

- Question 1.1: What information is to be collected?
- Incomplete Answer: The agency will collect information for a background check.
- More helpful answer: The Background Check System will collect the following: full name, date of birth, social security number, current address, phone number, 10 fingerprints AND results of the commercial data verification AND results of the background check

Homeland Security

# Section 1.0 Info. Collected & Maintained

- Question 1.2 From whom is the information to be collected?
- Incomplete Answer: The agency will collect information directly from the individual.
- More Helpful Answer: The agency will collect name, home address, and home telephone directly from the individual. The name and home address will be checked against a commercial aggregator to confirm the accuracy of the information.  Fingerprint verification checks are received back from the FBI.

Homeland Security

# Question 1.3 Why is the information being collected?

- Incomplete Answer: The agency is collecting the information to conduct a background check.
- More Helpful Answer: The agency is collecting name, date of birth, social security number, and current home address and telephone number in order to determine an individual's identity and compare it to known terrorists. The agency is collecting 10 fingerprints in order to determine your criminal history. The agency receives data from commercial data sources to verify home address. This information taken together allows the agency to conduct a full background check.

Homeland Security

# Section 1.0 Privacy Impact Analysis

- Do Not Delete This Section
- Analyze the answers to the previous questions, don't just restate the answers to them.

Homeland Security

# Section 1.0 Privacy Impact Analysis

- Identify the privacy risks related to
  - The scope of information collected
  - The sources of the collected information
  - The reasons for the collection
- Discuss possible mitigation
  - Reduce amount of information collected
  - Collect information directly from the individual
  - Build procedures and processes for identifying inaccurate information.

Homeland Security

# Section 2.0

- Uses of the System and the Information

# Section 2.2

- Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern?

Homeland Security

# Section 2.0 Privacy Impact Analysis

Look broader than the Accuracy Question.

- **Privacy Risks**
  - Use of information for undisclosed purposes
  - Inappropriate use
  - Automatic attribution of data mining information without human intervention
  - Inaccurate Information
- **Mitigation**
  - Review of public and privacy documentation
  - Security and access controls
  - Training on handling of personal information
  - Human review of data mining results
  - Direct collection of information and follow up prior to a decision if information appears inaccurate

# Section 3.0 Retention

- Privacy Impact Analysis
- Hypothetical

Homeland Security

# Section 4.0 Internal Sharing

## Privacy Impact

- Privacy Risks
  - Use of information for undisclosed purposes
  - Inappropriate or misuse of information
  - Misconstrued information
- Mitigation
  - Review of public information and privacy documentation to ensure transparency
  - Access and security controls
  - Training

Homeland Security

# Section 5.0 External Sharing

- If you have a SORN, Do NOT list the routine uses.

# Section 5.0 External Sharing

- Question 5.1: With which external organization is the information shared?
- FBI and Commercial Data vendors

Homeland Security

# Section 5.0 External Sharing

- Question 5.2: What information is shared and for what purposes?
- FBI: sharing name, date of birth and fingerprints for criminal history check.
- Commercial Data Vendors: sharing full name and address for address verification.

Homeland Security

# Section 5.0 Privacy Impact Analysis

- Privacy Risks
  - Information not secured by external partner
  - Information used for other purposes by external partners
  - Inappropriate use by external partners
- Mitigation
  - Written assurances that information is secured in conformance with FISMA
  - Information not maintained by external partner after query.
  - Written agreement how information will be collected, used, and maintained.

Homeland Security

# Section 6.0 Notice

- Privacy Impact Analysis
- Hypothetical

Homeland Security

# Section 7.0 Individual Access, Redress and Correction

- Privacy Impact Section
- Hypothetical

Homeland Security

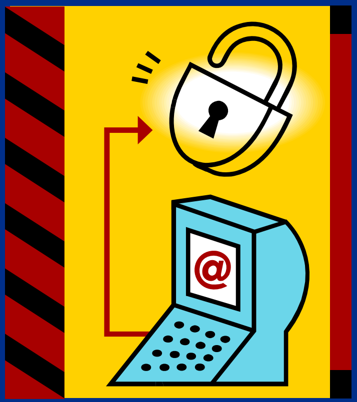
# Section 7.0 Individual Access, Redress and Correction

- Question 7.1 What are the procedures which allow individuals to gain access to their own information?
- Individuals may request access to their information by submitting a Freedom of Information Act/Privacy Act (FOIA/PA) request to XXX in writing by mail to the following address:
- Component Name
- FOIA Division
- ADDRESS FOR FOIA's

Homeland Security

# Section 8.0 Technical Access and Security

- Privacy Impact Analysis
- Hypothetical



# Section 9.0 Technology

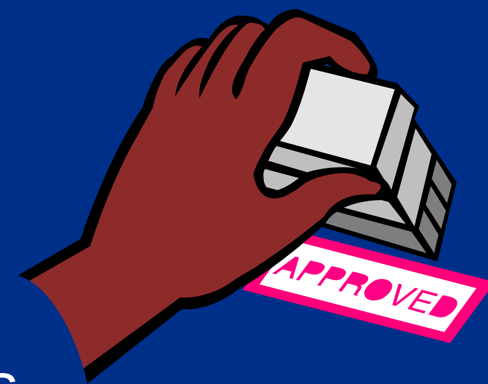
- How did you make your technology decisions in light of privacy protection?

# Conclusion

- Short description of privacy risks and mitigation strategies.

# PIA Review and Approval Process

- Email draft to
  - PIA@dhs.gov or
  - Rebecca.Richards@dhs.gov and Nathan.Coleman1@dhs.gov.




- We will review and provide comments.
- No response DOES NOT EQUAL approval
- Multiple collaborative iterations
- All PIAs are approved by Acting Chief Privacy Officer, Maureen Cooney
- Most will be published on the DHS website.

Homeland Security

# DHS Privacy Impact Assessment (PIA) Workshop

Thank you for attending

# Operationalizing Privacy

## Compliance Frameworks & Privacy Impact Assessments

Homeland Security

The Privacy Office

U.S. Department of Homeland Security
Washington, DC 20528
t: 571-227-3813; f: 571-227-4171
privacy@dhs.gov; www.dhs.gov/privacy