



Homeland  
Security

Privacy Office

Protecting privacy while promoting transparency



# *Privacy Threshold Analysis*

Dianna Carr

Privacy Analyst

---

Jameson Morgan

Privacy Compliance Analyst

# What is your job function?

- A. Privacy
- B. Security
- C. Legal
- D. FOIA
- E. Other
- F. I'm in the wrong room



# Had you heard of a PTA before today?

A. Yes

B. No



**Homeland  
Security**

| Privacy Office

# Does your agency use the PTA?

A. Yes

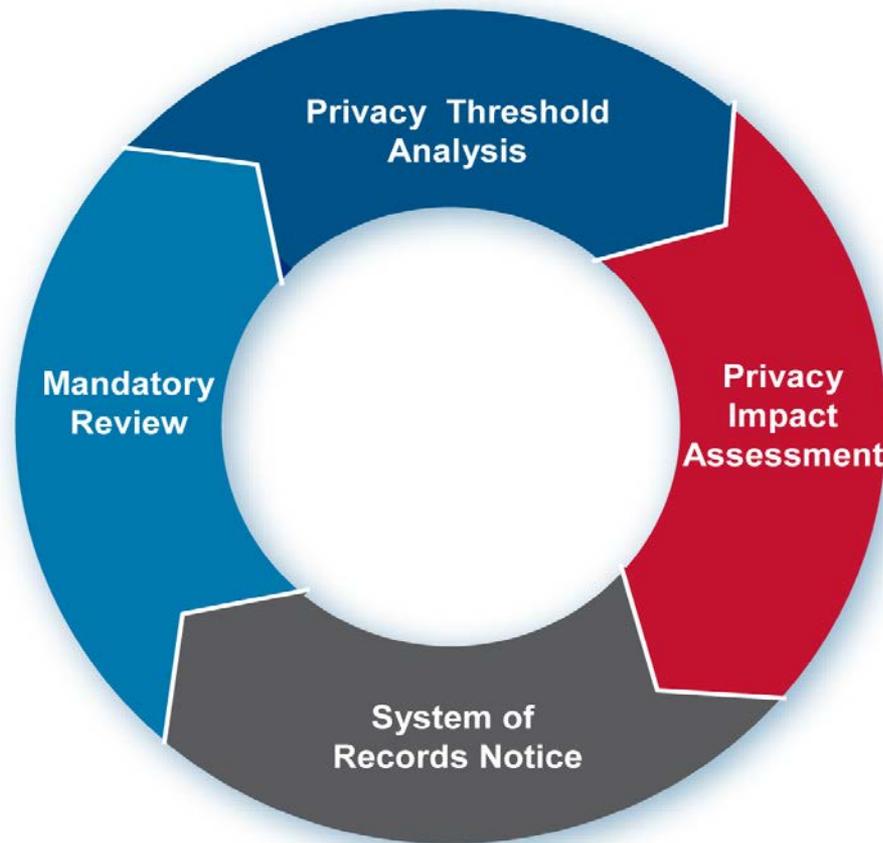
B. No



**Homeland  
Security**

| Privacy Office

# *Privacy Compliance Process*



# *What is a PTA?*

- A document that serves as the official determination by the DHS Privacy Office if a system, program, or project has privacy implications and if additional privacy compliance documentation is required:
  - Privacy Impact Assessment (PIA)
  - System of Records Notice (SORN)
- Templates can be found on our website at: <http://www.dhs.gov/privacy-compliance>



# *Why is a PTA completed?*

- To demonstrate that privacy has been considered during the review of any new or updated program, project, process, or technology.
- To provide a record of a privacy-sensitive system and its privacy requirements in our tracking database.
- To demonstrate compliance with privacy laws and regulations as required by the Office of Inspector General (OIG) and Government Accountability Office (GAO) during reviews.



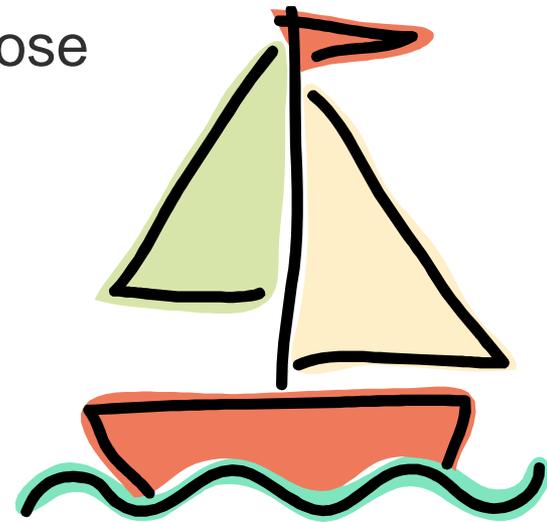
# *What are the benefits of a PTA?*

1. To determine if a system is privacy sensitive;
2. To better understand programs, pilots, systems, and sharing agreements; and
3. To build relationships throughout the agency.



# *When to do a PTA*

- For a new project
- For IT security
- When a project changes
  - Collects new PII
  - Uses the PII for a different purpose
  - Reduction of PII
- Every three years



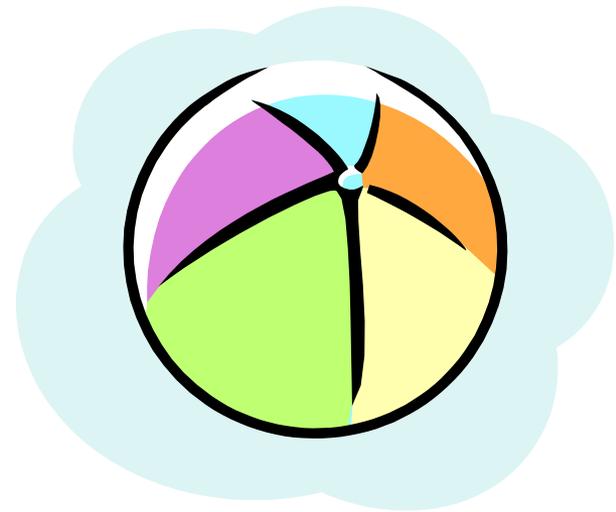
# *What are common PTA triggers?*

- Development or procurement of any new program or system that will handle or collect personally identifiable information (PII)
- Creation of new forms or other collections of PII (including but not limited to collections that trigger the Paperwork Reduction Act (PRA))
- Establishment of pilots that will use PII
- Development of program or system revisions that affect PII
- Issuance of a new or updated rulemaking that involves the collection, use, and maintenance of PII
- Initiation of a new information sharing of PII, whether internal or external
- Implementation of new uses of social media



# *Who is responsible for PTAs at DHS?*

- Component ISSOs\*/Program Managers
- Component Privacy Officers/Privacy Points of Contact (PPOCs)
- DHS Privacy Office



\* Information System Security Officer



**Homeland  
Security**

| Privacy Office

# *Types of DHS PTAs*

- Regular PTA
- Contacts List PTA
- Web Portals PTA
- Closed Circuit Television (CCTV) PTA
- Social Media PTA
- PTA Disposition



# *PTA questions*

1. Please describe the purpose of the project or program.
2. Project or program status (choices: existing, new, pilot or update)
  - a. Date first developed
  - b. Date last updated
  - c. Pilot launch date
  - d. Pilot end date
3. From whom does the project or program collect, maintain, use or disseminate information? (check all that apply: employees, contractors, members of the public and/or this program does not collect any PII)



# *PTA questions (continued)*

4. What specific information about individuals could be collected, generated or retained?
  - a. Does the project or program use Social Security Numbers (SSNs)?
  - b. If yes, please provide the legal authority for the collection of SSNs.
  - c. If yes, please describe the uses of the SSNs within the project or program.
  
5. Does this system employ any of the following technologies? (choices: Closed Circuit Television (CCTV), SharePoint-as-a-Service, Social Media, Mobile Application (or GPS), Web Portal, or none of the above)
  - a. If this project is a technology/system, does it relate solely to infrastructure?
  - b. If header or payload data is stored in the communication traffic log, please detail the data elements stored.



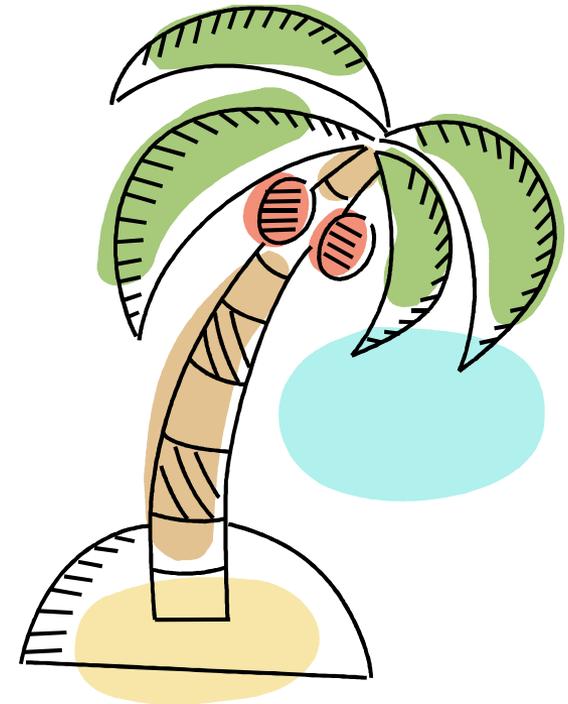
# *PTA questions (continued)*

6. Does this project or program connect, receive, or share PII with any other DHS programs or systems?
7. Does this project or program connect, receive, or share PII with any external (non-DHS) partners or systems?
  - a. Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?



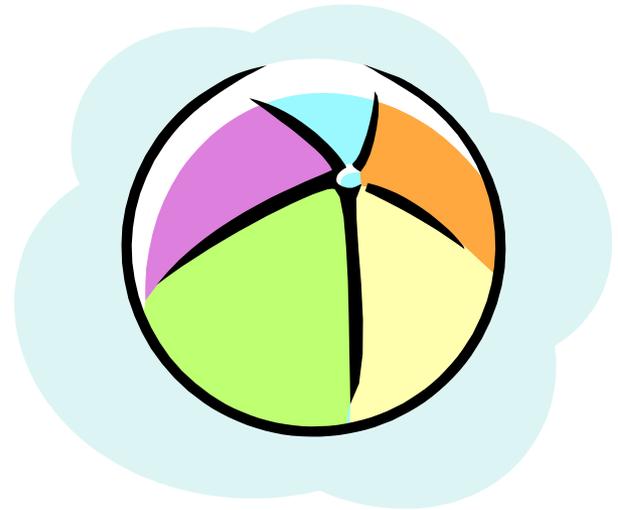
# *Adjudication page in depth*

- This is NOT a Privacy Sensitive System
  - No PII → No PIA or SORN required
- This is a Privacy Sensitive System
  - PII → further coverage is required
- Categories of Systems
  - IT System
  - National Security System (classified)
  - Legacy System
  - HR System (HR only)
  - Rule
  - Privacy Act Statement
  - Other



# *Adjudication page in depth (continued)*

- Determination
  - PTA sufficient at this time
  - Privacy compliance documentation determination in progress
  - New information sharing arrangement is required
  - DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies
  - Privacy Act Statement required
  - PIA is required
  - SORN required



# *Adjudication page in depth (continued)*

- PIA
  - System covered by existing PIA
  - New PIA is required
  - PIA update is required
- SORN
  - System covered by existing SORN
  - New SORN is required
  - SORN update is required
- DHS Privacy Office comments



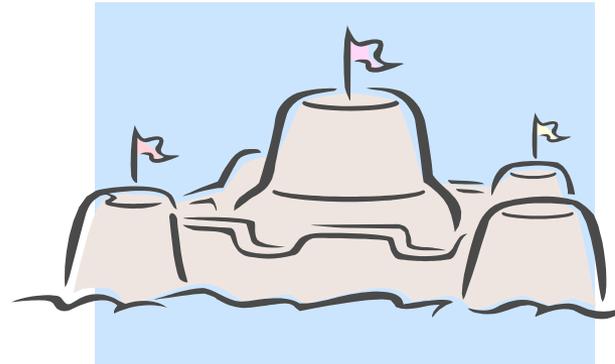
# *DHS Privacy Office responsibility*

- Review and adjudicate PTAs, including a description of the rationale for the privacy compliance determination
- Contact the component privacy officer/PPOC if additional information is needed
- Send final version of the PTA to the component



# *Why should your organization use the PTA?*

- Assists in determining privacy-sensitive systems, processes, and programs
- Easy to use format
- Provides better understanding to your Privacy Office
- Memorializes privacy documentation determinations



# Question 1: Which of the following is NOT a reason to complete a PTA?

- A. To demonstrate that privacy has been considered during the review of any new or updated program, project, process, or technology.
- B. To provide a record of a privacy-sensitive system and its privacy requirements.
- C. Because it is required by the Privacy Act of 1974.
- D. To demonstrate compliance with privacy laws and regulations.



## Question 2: Which is NOT a benefit of a PTA?

- A. To determine if a system is privacy sensitive.
- B. To provide legal protection for your agency.
- C. To better understand programs, pilots, systems, and sharing agreements.
- D. To build relationships throughout the agency.



## Question 3: Which is NOT a reason to perform a PTA?

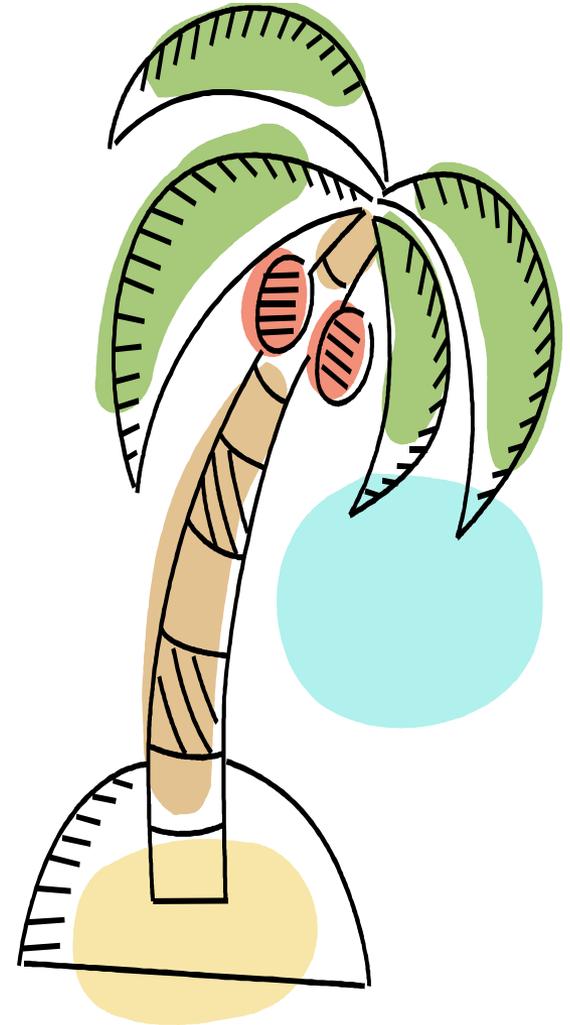
- A. For a new project
- B. For IT security
- C. When a project changes
- D. Every three years
- E. When the information system security officer (ISSO) or program manager (PM) change



# Resources

For more information:

- Visit our website for templates and guidance:
  - [www.dhs.gov/privacy](http://www.dhs.gov/privacy)
- Email us:
  - [privacy@dhs.gov](mailto:privacy@dhs.gov)





**WHO**

**WHAT**

**WHERE**

**WHEN**

**WHY**

**HOW**

**QUESTIONS**

**ANSWERS**



Homeland  
Security

Privacy Office

Protecting privacy while promoting transparency



# *Privacy Impact Assessments*

Debra Danisek

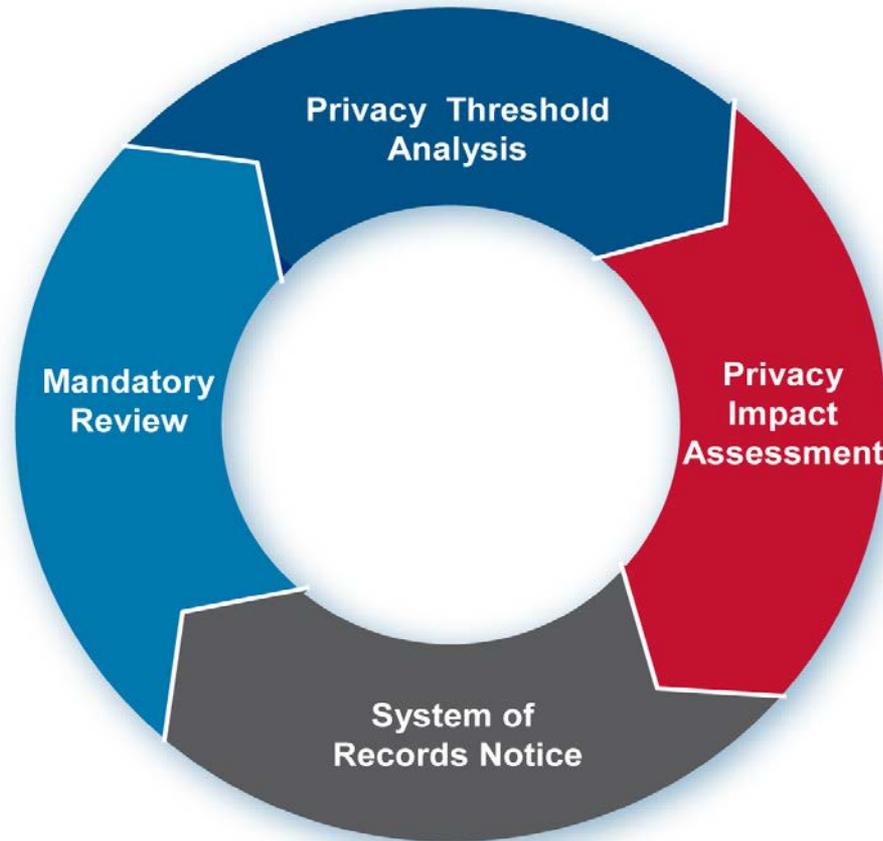
Associate Director for Privacy Compliance

---

Dayo Simms

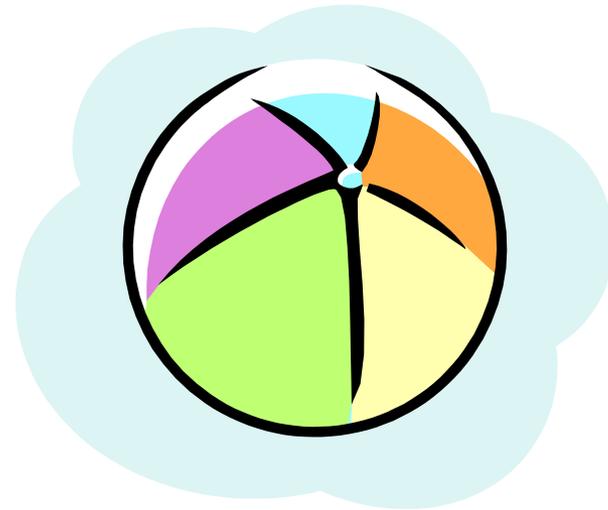
Privacy Compliance Analyst

# *Privacy Compliance Process*



# *Privacy Impact Assessments*

- A successful PIA should accomplish two goals:
  - Determine the risks and effects; and
  - Evaluate protections and alternative processes to mitigate potential privacy risks.



# *Conduct a PIA when...*

- Developing or procuring any new technologies or systems that handle or collect PII.
- Developing system revisions that contribute to new privacy risks.
- Issuing a new or updated rulemaking that entails the collection of PII.
  - *Even if a component has specific legal authority to collect certain information or build a certain program or system, a PIA is required.*



# Is a PIA required?

	E-Gov Act	OMB 03-22	HSA 222	DHS 2008-02
Electronic collection, use, maintenance, dissemination from U.S. citizens/LPRs	X	X	X	X
Elevated privacy risk, even if not IT		X		X
Rulemakings that elevate privacy risk			X	X
Collections from non-U.S. citizens/LPRs				X
Any technology, rulemaking, program or activity (including pilots)				X
Employee information only, if Department-wide program				X



# *Types of DHS PIAs*

- Standard information technology PIAs
- Rulemaking PIAs
- Human Resource PIAs
- National Security System PIAs
- Program PIAs
- Privacy Sensitive Technology PIAs
- Pilot Testing PIAs



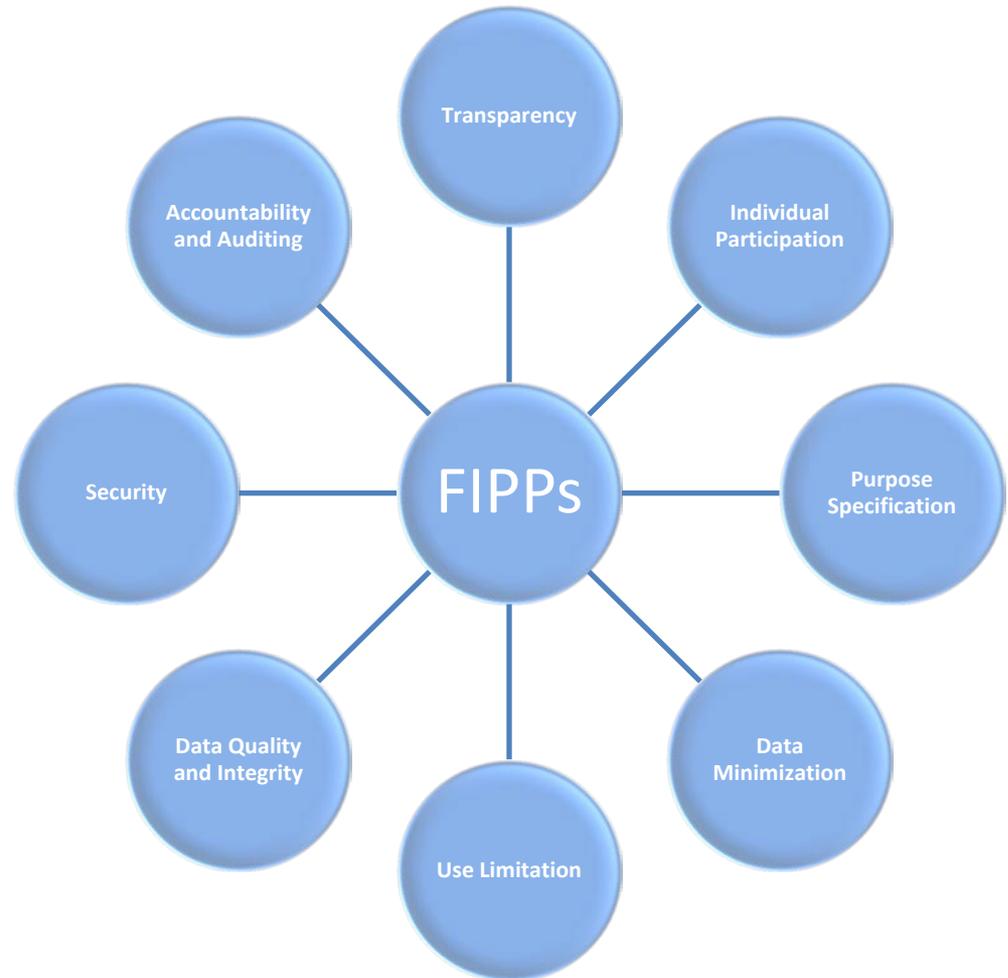
# *When is a PIA NOT required by DHS?*

- No PII collected and an adjudicated PTA from the Privacy Office
- HR systems that only collect on one component
- Already have an existing PIA and changes don't require an update



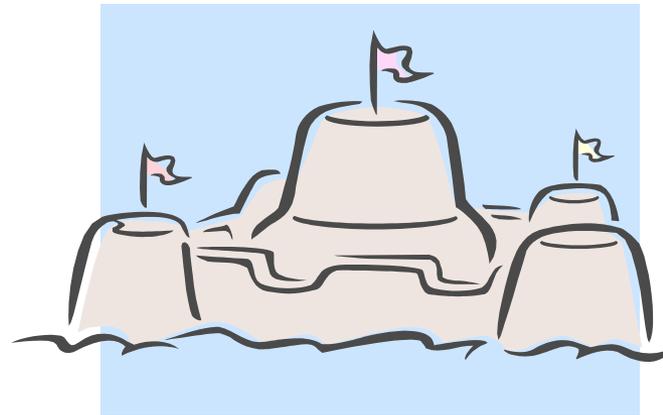
# *Fair Information Practice Principles*

- Transparency
- Individual Participation
- Purpose Specification
- Data Minimization
- Use Limitation
- Data Quality and Integrity
- Security
- Accountability and Auditing



# *Overview of the Program*

- What does the PIA cover?
- Why are you collecting PII?
- Typical transaction
- Identify major privacy risks and ways to mitigate them



# Section 1.0 Authorities and Other Requirements

- **Legal authorities:**
  - Explain how the **statutory and regulatory authority** permits the project and the collection of the subject information.
  - The **Privacy Act is NOT an authority** for collection of PII.
- **Privacy Act Coverage:**
  - List appropriate **SORN and citation**, check forms for appropriate e(3) statements
- **Other Compliance Areas:**
  - System Security Plan, Records Retention Schedule, Paperwork Reduction Act requirements

**FIPPs:**  
*Purpose Specification*



## *Section 2.0 Characterization of the Information*

- Data elements collected by the system
- Sources of the information, and how was the information collected
- Accuracy of data

### **FIPPs:**

- *Purpose Specification*
- *Data Minimization*
- *Individual Participation*
- *Data Quality and Integrity*



# Section 3.0 Uses of the Information

- **Use vs. Purpose**

- Purpose is the program or mission objective requiring the information and is directly connected to the statutory authority for the agency program.
- Uses are the specific ways or operations (usually repetitive in nature) in which the information is processed.

- **How is the information used by DHS?**

- Is the data queried for patterns? Is new information produced? Is there intra-agency sharing?

**FIPPs:**

- *Use Limitation*
- *Transparency*



# Section 4.0 Notice

- Describe how notice offered to individuals is reasonable and adequate in relation to the system's purpose and uses, the sensitivity of the PII, the capabilities for notice permissible within the system's design, and the limitations (e.g., Privacy Act exemptions) required by law or mission necessity.

## FIPPs:

- *Transparency*
- *Use Limitation*
- *Individual Participation*



# *Section 5.0 Data Retention by the Project*

- Retention schedules should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act.
  - The schedule should align with the stated purpose and mission of the system.

## **FIPPs:**

- *Data Minimization*
- *Data Quality and Integrity*
  - *Security*



# *Section 6.0 Information Sharing*

- Describes what is shared EXTERNALLY, for what purpose, with whom, and when
  - Applicable routine uses

## **FIPPs:**

- *Use Limitation*
- *Data Quality and Integrity*
  - *Security*



# *Section 7.0 Redress*

- Provides information on individual access and how to correct a record about him/herself
- Describes procedures that are in place other than the Privacy Act/FOIA request route
- Informs how individuals are notified of these procedures

**FIPPs:**  
*Individual Participation*



# *Section 8.0 Auditing and Accountability*

- Describe what controls determine which persons may access the system and the extent of their access, and what monitoring, recording, and auditing safeguards are in place to prevent or detect unauthorized access or inappropriate usage.

**FIPPs:**  
*Accountability and Auditing*



# *Department-wide PIAs*

- **DHS-wide PIAs**

- Contact Lists
- SharePoint
- CCTV
- Complete a specialized PTA. If the program adheres to the rules, it will be covered by the appropriate DHS-Wide PIA and added to the Appendix.
- DHS Web Portals
- Social Media

- **PIA Update Template**

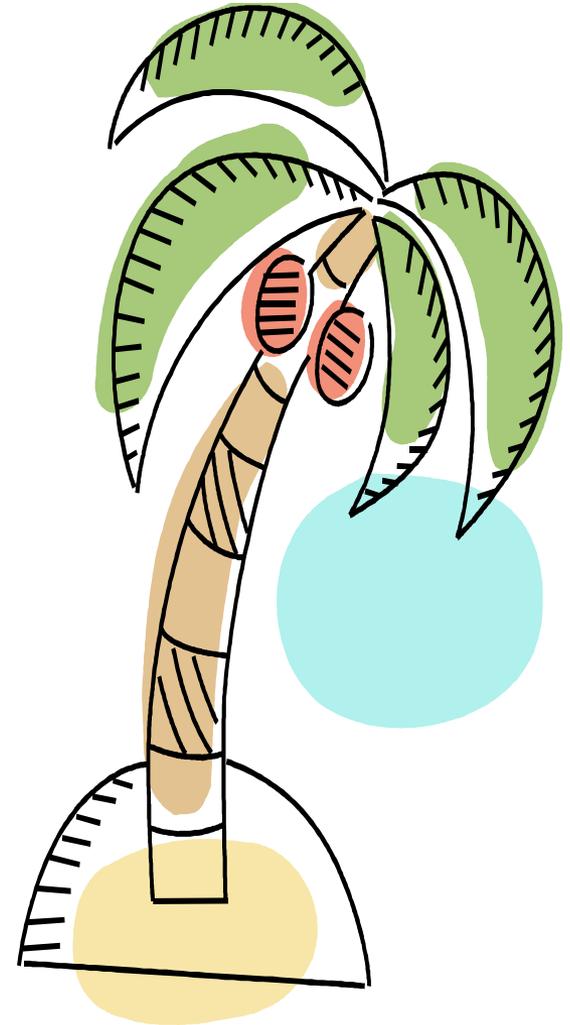
- **Three-year PIA checklist**



# Resources

Visit [www.dhs.gov/privacy](http://www.dhs.gov/privacy) for:

- Templates and Guidance:
  - PTA
  - PIA
  - SORN
  - NPRM/Final Rule
  - Privacy Act Statement
- Privacy Policy Guidance Memoranda



# Question 1: If the system collects too much data, privacy mitigation should include:

- A. Data accuracy
- B. Collect more data
- C. Collect only necessary data
- D. Share all data



## Question 2: Publishing a PIA online meets the following FIPPS *except*?

- A. Transparency
- B. Accountability and Auditing
- C. Individual Participation





**WHO**

**WHAT**

**WHERE**

**WHEN**

**WHY**

**HOW**

**QUESTIONS**

**ANSWERS**



Homeland  
Security

Privacy Office

Protecting privacy while promoting transparency



# *System of Records Notice Privacy Act Disclosures*

Nathan Wildermann

---

Deputy Privacy Officer,  
Immigration & Customs Enforcement

# *Privacy Act – What it applies to*

- **Applies to:**
  - Federal agency records only
  - Paper or Electronic
  - Citizens and LPRs
  - Aliens per DHS policy
  
- **Does not apply to:**
  - Deceased persons
  - States, private companies



# *Privacy Act – What it applies to*

- **Record:** Information (1) about an individual (ex. medical, criminal, or employment history); that is, (2) maintained by or on behalf of an agency; and, (3) contains the individual's name or other identifier (SSN, fingerprint, A-Number).
- **System of Records:** Any group of records under the control of an agency from which information is retrieved by the name of the individual or other identifier.



# *Privacy Act – What it applies to*

- Most DHS records about individuals are in a system of records and covered by the Privacy Act
- Exception:
  - Record systems where you pull records only by date, subject, etc.



# *Sharing Privacy Act Data*

Privacy Act of 1974 (5 U.S.C. § 552a) – Subsection (b)

- Always permitted with written consent
  - ICE Privacy Waiver (Form 60-001)
- Permitted disclosures most relevant to ICE:
  - (b)(1) Within agency for official purposes
  - (b)(3) When SORN “routine use” allows the disclosure
  - (b)(7) Law enforcement request
  - (b)(9) When requested by Committee or Subcommittee of Congress
  - (b)(11) By Federal court order (Article III)



# *(b)(7) Authority Disclosures*

- 5 USC § 552a(b)(7) – request for records in support of LE investigation or activity
- Must be a written request signed by head of LE agency or delegate.
  - Domestic agencies only
  - Criminal, civil or administrative LE
  - Must request specific records – no fishing!
- ICE can receive or make (b)(7) requests!
- **See** Privacy Office (b)(7) Guidance for sample letters, more help
- If (b)(7) does not allow disclosure, look for a routine use!



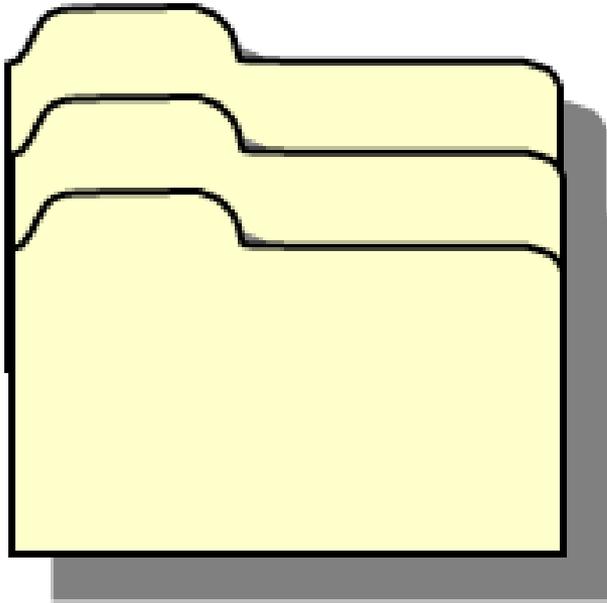
# *Purpose of the SORN*

- SORNs are legally binding, and:
  - Describe an agency’s “system of records” and the way that the agency collects, maintains, uses, and disseminates personal information about individuals.
  - Publish in *Federal Register* for public comment
  - Cover both paper and electronic records
  - Educate the public, promotes transparency, and ensures government accountability



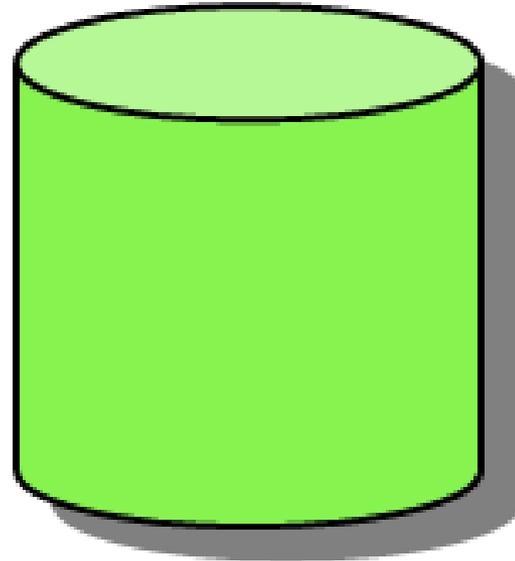
# *SORN and IT System Mapping*

## **Paper Records**

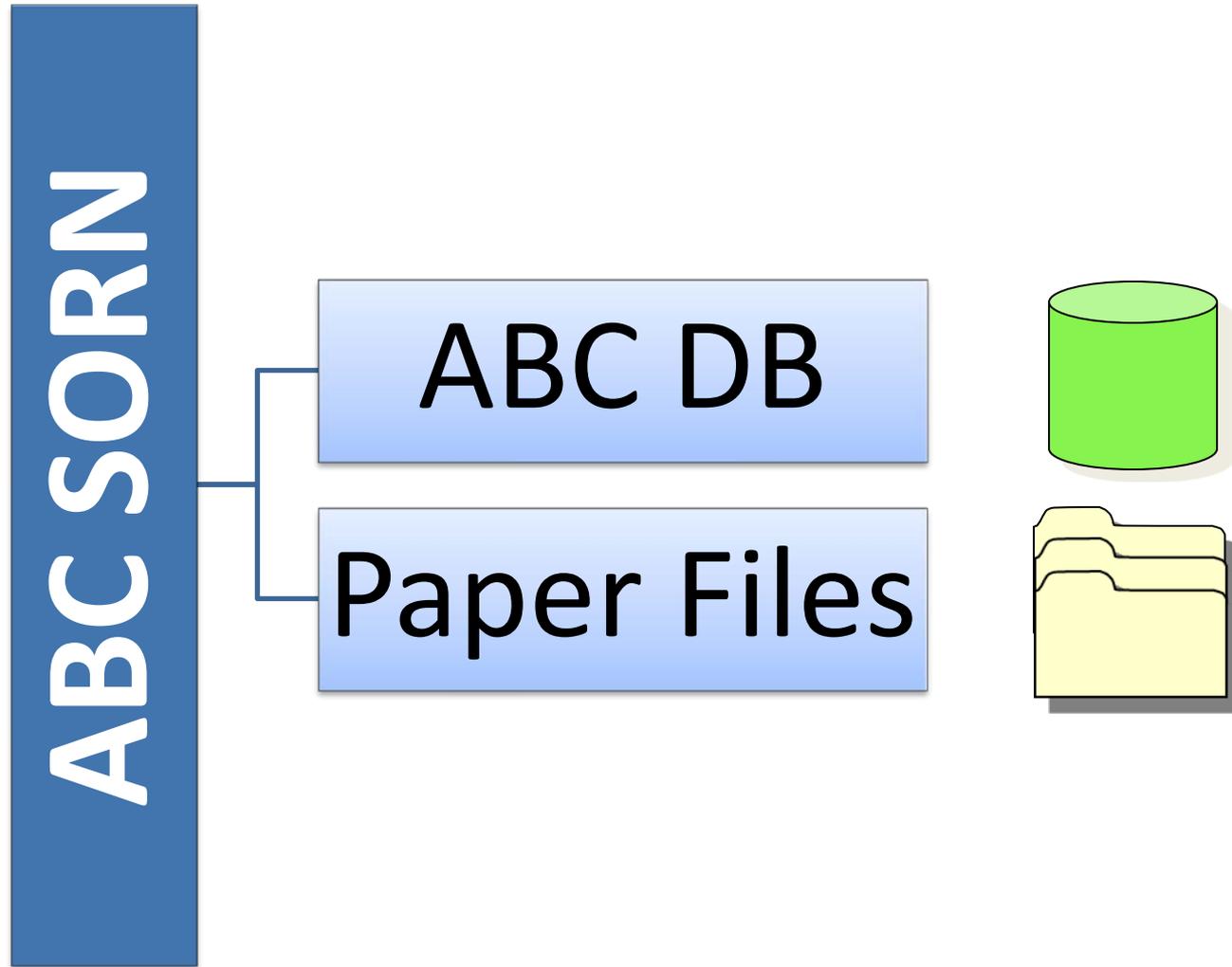


## **Electronic Records**

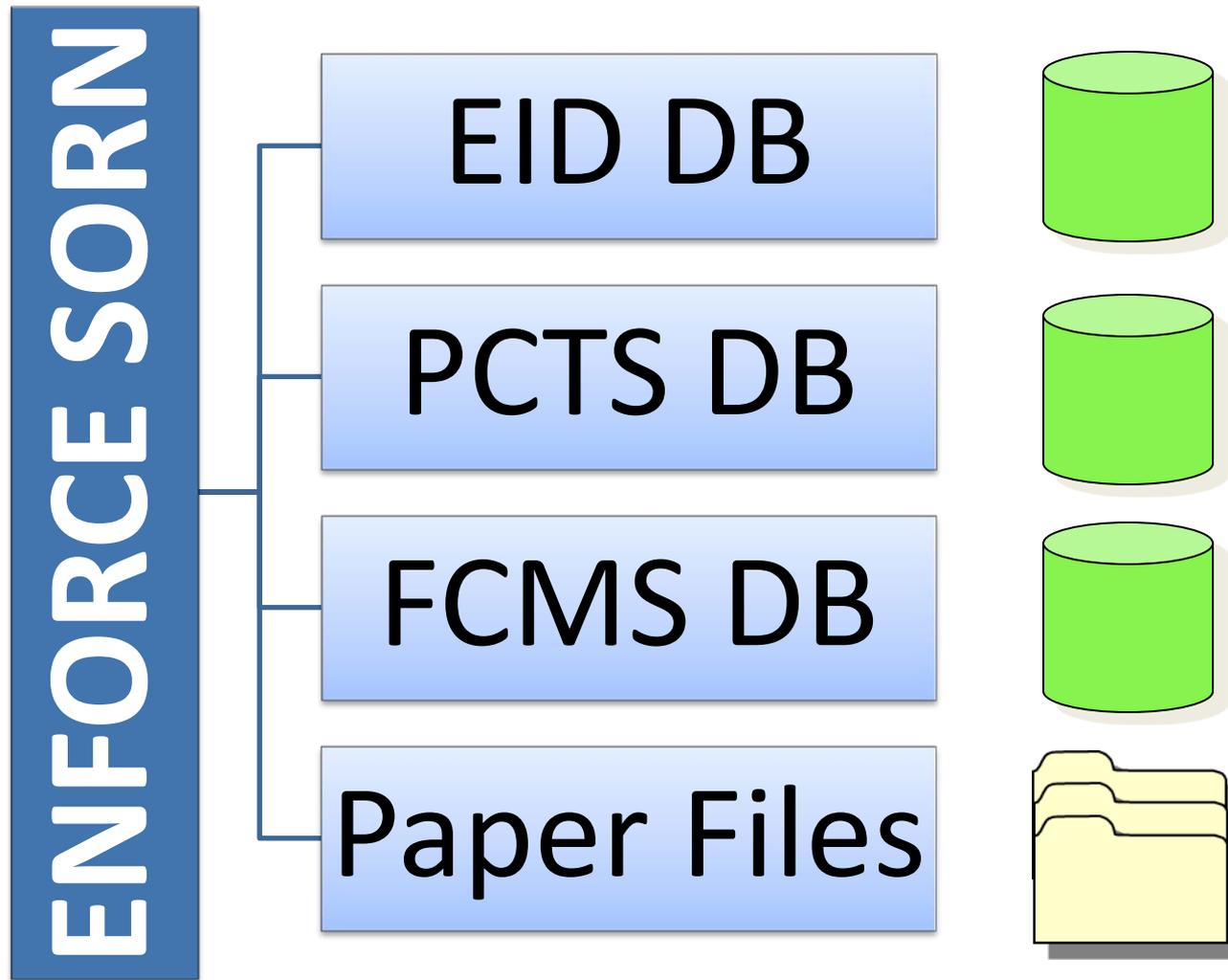
- Databases
- Electronic Storage



# *SORN and IT System Mapping*



# *SORN and IT System Mapping*



# *Anatomy of a SORN*

- Introduction
- System Name/#
- Security Classification
- Location
- Individuals
- Data
- Authorities
- Purposes
- Routine Uses

- Storage, Retrieval & Safeguards
- Retention
- System Manager
- Notification
- Access
- Amendment
- Sources
- Exemptions Claimed
- Signature



# *Other Disclosure Restrictions*

## **Immigration Related**

- Information Relating to Persons Filing Claims Under Violence Against Women Act Claimants (VAWA)
- Battered Spouse or Child Information
- Asylum, Refugee, Withholding of Removal, Protection Under Convention Against Torture, and Credible Fear / Reasonable Fear Determination Information
- T Visas and U Visas



# *Other Disclosure Restrictions*

## **Additional Restrictions**

- Critical Infrastructure Information
- Child Victim/Witness Information
- Title III Wire Intercept Information
- Classified Information



# *Privacy Act Disclosure Rules*

## Accounting for Disclosures

- Keep track of all disclosures made from a person's Privacy Act file, except for intra-agency disclosures & FOIA disclosures
- Accountings must contain:
  - Date, nature and purpose of each disclosure
  - Name and address of the person/agency recipient
- Individual right to access their own records and a copy of the accounting
  - Exceptions for law enforcement/national security.



# *Scenarios*



**Homeland  
Security**

| Privacy Office



**WHO**

**WHAT**

**WHERE**

**WHEN**

**WHY**

**HOW**

**QUESTIONS**

**ANSWERS**



# *Information Sharing Panel Discussion*

## Panelists:

- Ken Hunt, *Acting Senior Director, Privacy Policy*
- Lauren Saadat, *Director, International Privacy*

## Moderator:

Akbar Siddiqui, *Attorney Advisor,  
U.S. Customs and Border Protection*

# Information Sharing: The Role for Privacy Officials

- Information sharing is where Compliance meets policy
  - *(the interplay between “may” and “should”)*



# *Privacy's Role*

- *Support Information Sharing Infrastructure:*
  - Physical: Component-, agency-, government-wide
  - Policy: How can sharing implement the FIPPs?
  - Agreement process: consult, negotiate, draft, review
  - Post agreement: train, audit, support transparency



# *Types of Information Sharing*

- Internal vs. External
- Domestic vs. International
- Inbound vs. Outbound vs. Two-Way
- Data Delivery Scope/Method
  - Track 1 – Account Access
  - Track 2 – Requests for Information
  - Track 3 – Bulk Sharing for Ingest



# *First: Common Considerations*

- Compliance Review – Is the disclosure consistent with the SORN and PIA?
- How must the transaction be memorialized?
  - MOUs, LOIs, etc.
- However accomplished...does the data exchange implement the FIPPs?



# *Account Access*

- DHS Privacy Office reviews ISAAs.
- ISAAs often include privacy training and audit controls as a condition of gaining and maintaining access.
- Define how user is able to change records or acquire information gained from account access into a new system.



# *Requests for Information*

- Generally, the least privacy intrusive sharing
- Still, DHS PRIV reviews some of them:
  - Consistent with compliance documentation
  - Lawful purpose
  - Appropriately scoped
  - PII minimized



# *Bulk Sharing*

## *Inherent Privacy Risks:*

- Data Quality – copy of the data, correction
- Redress
- Use Limitation – once it's gone, it's gone
- Typically undifferentiated “good guy” data
  - Mixed USPER/nonUSPER, a further complication



# *Bulk Sharing Case Study - NCTC*

- DHS shares with NCTC under all three tracks.
- DHS and NCTC have five ISAAs authorizing bulk sharing:
  - APIS, ADIS, ESTA, RAPS, and SEVIS



# *Bulk Sharing with NCTC (con't)*

- DHS established the Records Working Group to consolidate interaction with NCTC:
  - I&A, OGC, PRIV, CRCL, PLCY, Components
  - Advise S1 on framework for sharing data set by data set
  - Negotiate terms and conditions with NCTC
  - Provide Transparency
  - Monitor compliance



# *Bulk Sharing with NCTC (con't)*

## *Initial Considerations:*

- Sharing benefits both parties – evaluate the Use Cases
- Track 3 only method of satisfying identified Use
- Privacy Compliance Review
  - Consistent with the purpose - Counterterrorism
  - Routine Use
  - Consistent with PIA



# *Bulk Sharing with NCTC (con't)*

## *Key Provisions:*

- Define Users and Uses
- Define (Temporary) Retention period (and how data becomes suitable for Permanent Retention)
- Account for all data (USPERs, Asylum seekers, other special protected classes) – handling, training, minimize
- Wrap back – benefit to DHS
- Restricts onward sharing
- Reporting and Audit
- Transparency



# *NCTC – “Gold Standard” Protections*

- Temporary retention - data set by data set
- Onsite Oversight Representative
- Additional transparency
- Additional redress
- No distinction between USPER and Non-USPER
- Termination for cause



# *Final Thoughts*

- Information Sharing Infrastructure
- Physical: RWG, ISSGB, ISCC, CVTF, ISE governance
- Policy: Bulk Sharing Principles, ISAA Guidebook, NCTC framework of factors
- Agreement process: consult, negotiate, draft, review
- Post agreement: train, audit, support transparency

FIPPS

TRANSPARENCY



**Homeland  
Security**

| Privacy Office

# *How Are International ISAAs Initiated?*

- Broad policy, often multilateral or by statute
  - examples: 5CC, PCSC, BTB
- OIA's International Affairs Engagement Plan



# *Authorities for Leading and Coordination*

- OneDHS: International ISAAs must be drafted at the Department level
- IAGB Charter: IAGB must lead and coordinate all international agreements
- ISSGB Charter: ISSGB must approve of all ISAAs
- I&A Delegation and Directive: I&A must coordinate all ISAAs
- Privacy Compliance Directive: PRIV is responsible for ensuring international ISAAs comply with privacy compliance documentation and privacy policy



# *Terms of International ISAAs*

- Must be signed at HQ level
- Use of “domestic law” instead of clear terms
- Terms of art that only apply to one country’s legal framework
- Audit/Review
- Redress
- Notice
- Subordinate agreements necessary



# *Other Considerations*

- Public trust and confidence, both here and abroad, are essential to our international programs, yet policy leaders may overlook privacy.
- Coordination is key: project documentation (ISAA, PTA, PIA, SORN) must all be consistent.
- Winning the Beauty Contest





**WHO**

**WHAT**

**WHERE**

**WHEN**

**WHY**

**HOW**

**QUESTIONS**

**ANSWERS**



Homeland  
Security

Privacy Office

Protecting privacy while promoting transparency



# *Privacy Incident Response Best Practices*

Kate Claffie

---

Associate Director,  
Privacy Oversight

# *Topics*

- Why is Privacy Important?
- What is Personally Identifiable Information (PII)?
- What is Sensitive PII?
- Office of Management and Budget Guidance
- Privacy Incident Reporting at DHS
- Best Practices



# *Why is Privacy Important?*

- To earn and keep public trust
  - If the public no longer trusts DHS to protect their PII, public support for DHS programs may erode.
- To prevent privacy incidents
  - Incidents reported in national news erode the public's trust in those agencies, and are expensive to mitigate.
- To prevent identity theft
  - Privacy incidents that raise the risk of identity theft can be lengthy, costly, and stressful to recover from for the individual and DHS.
- It's the law
  - Failure to follow these laws may result in civil or criminal penalties, or loss of employment.



# *Personally Identifiable Information (PII)*

- Any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to an individual.
- DHS uses a broad definition of PII and extends privacy protections regardless of whether the individual is a U.S. Citizen, Legal Permanent Resident, or a visitor to the U.S.



# *Personally Identifiable Information (PII)*

PII includes:

- Name
- Date of Birth
- Mailing address, phone number, and/or email address
- Social Security number (SSN)
- Other Government-issued numbers (e.g., Passport, Alien Registration, driver's license)
- Account numbers
- Biometric identifiers



# *Sensitive PII*

- Potential for substantial harm, embarrassment, inconvenience, or unfairness to an individual if compromised
- Single data elements
  - Social Security number, driver's license or state identification number, Passport number, Alien Registration Number, or financial account number
- Combinations of data
  - citizenship or immigration status; medical information; ethnic, religious, sexual orientation; account passwords
- Context of data
  - a list of employees with poor performance ratings.



# Office of Management and Budget Guidance: The Foundation for Incident Reporting



# *Office of Management and Budget Guidance*

- OMB Memorandum 06-15, ***Safeguarding Personally Identifiable Information*** (May 22, 2006)
  - Emphasizes agency responsibilities to safeguard Sensitive PII and train employees on their responsibilities for protecting privacy.
- OMB Memorandum 06-19, ***Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*** (July 23, 2006)
  - Requires agencies to report all incidents (actual or potential) involving PII to US-CERT within one hour of discovery of the incident.



# *Office of Management and Budget Guidance*

- OMB Memorandum, ***Recommendations for Identity Theft Related Data Breach Notification*** (September 20, 2006)
  - Provides recommendations from the President's Identity Theft Task Force to develop planning and response procedures addressing PII incidents that could result in identify theft.
- OMB Memorandum 07-16, ***Safeguarding Against and Responding to the Breach of Personally Identifiable Information*** (May 22, 2007)
  - Each agency must develop an incident response plan.
  - Sets requirements for remote access and portable devices.
  - Requires development of policies and procedures for reporting and mitigating PII incidents, and for notification of privacy incidents (actual or potential) to US-CERT within one hour of discovery.



# Privacy Incident Reporting at DHS



**Homeland  
Security**

| Privacy Office

# *What is a Privacy Incident?*

- The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any other situation where persons other than authorized users have access or potential access to PII in usable form, or where authorized users access PII for an unauthorized purpose.
- Involves PII in physical (hard copy) or electronic form.
- Includes suspected or confirmed privacy incidents.



# *Types of Harms Resulting from a Privacy Incident*

- Harm to an Agency:
  - Undermining the integrity or security of a system or program
  - Embarrassment
  - Reputation
- Harm to an individual:
  - Identity theft
  - Embarrassment
  - Harassment
  - Unfairness



# *Examples of Privacy Incidents*

- E-mail containing payroll information sent from a government e-mail account to a personal e-mail account.
- Theft of an unencrypted laptop containing benefit application information.
- Lost or stolen thumb drive or portable hard drive containing PII.
- E-mail containing Sensitive PII sent internally to an individual who had no need to know.
- A package of employee applications lost in the mail.
- Unauthorized access to personnel files.
- Documents containing PII thrown in a garbage can.



# *DHS Privacy Incident Handling Guidance (PIHG)*

- Developed in conjunction with:
  - DHS Chief Information Officer (CIO) and Chief Information Security Officer (CISO)
- Provides privacy incident identification and handling guidance
- Includes checklists for all stages of privacy incident handling
- Addresses all types of privacy incidents (paper, electronic, web-based, or physical occurrence)



# *DHS Privacy Incident Handling Guidance (PIHG)*

- Originally issued in September 2007
- Revised and reissued on January 26, 2012 to streamline processes and incorporate lessons learned since 2007
- DHS Security Operations Center (SOC) Standard Operating Procedures also include privacy incident reporting procedures



# *Reporting a Privacy Incident at DHS*

- Individual notifies Program Manager (PM) of potential or actual loss or disclosure of PII
- Or –
- PM and/or Component Privacy Officer/Privacy Point of Contact (PPOC) notifies component Information System Security Manager (ISSM) of potential or actual loss or disclosure of PII
- ISSM and/or PPOC completes initial Privacy Incident Report Template in the DHS SOC Online Reporting System



# *Reporting a Privacy Incident at DHS*

- DHS SOC Online notifies US-CERT and sends an automatic email alert message with initial Privacy Incident report to:
  - Component ISSM and Component Privacy Officer/PPOC
  - DHS Privacy Office Oversight Team
  - DHS Office of Inspector General
- If the privacy incident is significant, DHS SOC also notifies:
  - DHS Chief Privacy Officer
  - DHS Chief Information Officer (CIO) and Deputy CIO
  - DHS Chief Information Security Officer (CISO) and Deputy CISO
  - Component Head



# *Privacy Incident Handling – Steps*

- Component Privacy Officer or PPOC/ISSM performs the following steps for every privacy incident:
  - **Escalation** – identify who in the component’s management team should be notified, and whether outside entities need to be involved (e.g., local law enforcement, financial entities)
  - **Investigation** – conducted by the Component Privacy Officer or PPOC/ISSM, as well as by the OIG or law enforcement as warranted
  - **Notification** – evaluate need for notification of affected individuals of the actual or potential loss/compromise of PII
  - **Remediation** – determine corrective and protective actions to be taken to minimize loss and/or harm to individuals and Component/Department
  - **Closure** – recommend closure upon completion of mitigation/remediation of privacy incident



# *Risk Assessment: Five Factors*

- During the privacy incident handling process, these five factors are continuously reviewed as information is discovered:
  - Nature of data elements involved
  - Number of individuals affected
  - Likelihood that PII is accessible and usable
  - Likelihood that the privacy incident may lead to harm
  - Ability of Component to mitigate the risk of harm



# *Case Study*



**Homeland  
Security**

| Privacy Office

# *Final Closure of a Privacy Incident*

- DHS Privacy Office reviews all requests for closure of privacy incidents
  - DHS Privacy Office is the final decision maker
  - DHS Privacy Office updates the privacy incident report on DHS SOC Online to close an incident
  - DHS Privacy Office provides oversight for all privacy incidents and maintains statistical and historical data on incident reporting



# *Best Practices*

1. Constant communication between DHS Privacy Office, Component Privacy Officers/PPOCs, and DHS SOC
2. Regular Privacy Incident Handling Meetings
  - Provide statistics and highlight trends
  - Presentations on relevant topics (e.g., hacking, training)
3. Using anonymized examples for training
4. Leveraging expertise of DHS SOC for technical-related privacy incidents and emerging IT-related issues
5. Collaborating with staff on privacy training, tip sheets, and guidance related to privacy incidents
  - Incorporating privacy incident scenarios into mandatory privacy training



**Kathleen Claffie**

**Associate Director, Privacy Oversight**

DHS Privacy Office

[Kathleen.Claffie@hq.dhs.gov](mailto:Kathleen.Claffie@hq.dhs.gov)

202-343-1744



**Homeland  
Security**

| Privacy Office



**WHO**

**WHAT**

**WHERE**

**WHEN**

**WHY**

**HOW**

**QUESTIONS**

**ANSWERS**



Homeland  
Security

Privacy Office

Protecting privacy while promoting transparency



# *Privacy Compliance Reviews*

Martha Landesberg, Senior Director

---

Privacy Oversight  
DHS Privacy Office

# *Privacy Compliance Reviews at DHS*

- Consistent with the Privacy Office's unique position as both an advisor and an oversight body for the Department's privacy sensitive programs and systems, the Privacy Compliance Review (PCR) is designed to improve a program's ability to comply with assurances made in privacy compliance documentation (e.g., privacy policy, Privacy Impact Assessment).
- PCRs are a *constructive* mechanism to assess implementation of protections described in documentation, to identify areas for improvement, and to correct course if necessary.



# *What are the potential outcomes and benefits of a PCR?*

- Recommendations to the program resulting in improvements
- Updates to privacy documentation
- Informal discussions about lessons learned
- Formal report either internal or publicly available
- Heightened awareness by all participants about privacy
- Early issue identification and remediation





**WHO**

**WHAT**

**WHERE**

**WHEN**

**WHY**

**HOW**

**QUESTIONS**

**ANSWERS**

# Department of Homeland Security, Office of Inspector General Office of Information Technology, System Privacy Audit Division

Frank Deffer, Assistant Inspector General  
Marj Leaming, Director

Eun Suk Lee, Privacy Audit Manager  
Kevin Mullinix, Privacy Program Analyst  
Christopher Browning, Program Analyst

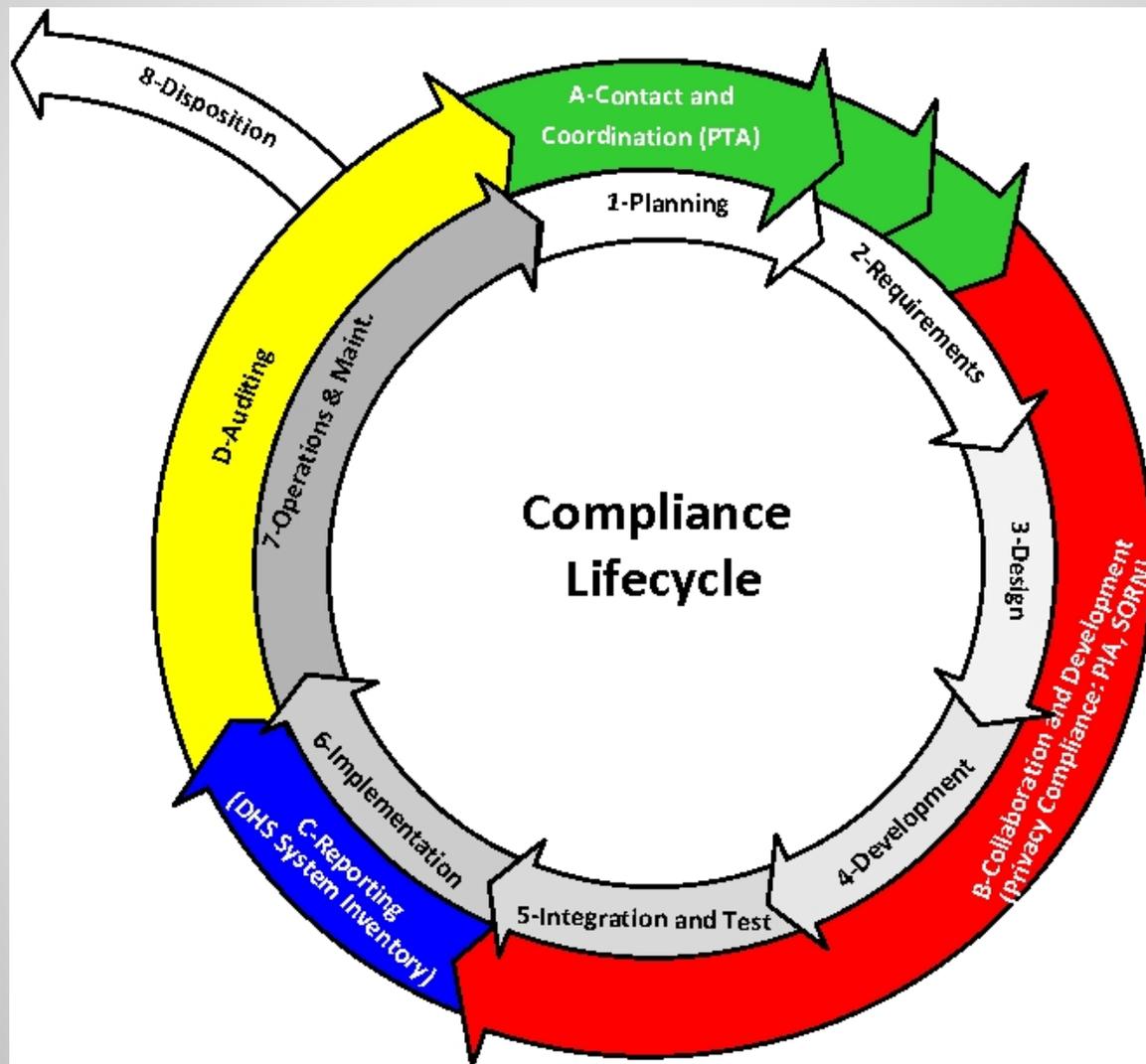
## Consistently Monitor Your Privacy Ecosystem

\*From [DHS-OIG Component Privacy Stewardship Audit series](#)

- **82** field site evaluations
- **553** managers interviews
- **662** privacy incidents analysis
- **204** SORs & **1175** compliance documents (PTA, PIA, SORN)
- **11** component surveys (242,322 employees with **14.25% response**)
- **24,962** unique comments on privacy risks and improvements

\*Insights from Peter Pietra, [Transportation Security Administration](#) Privacy Officer

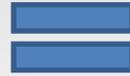
# Continuously Monitor Throughout the Life Cycle of Your Privacy Ecosystem



# What if an Incident Released 1 Terabyte of Privacy Data?

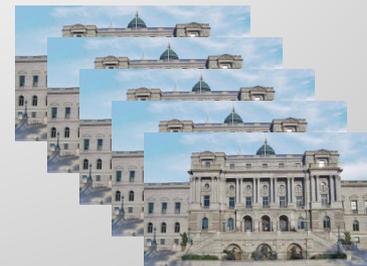
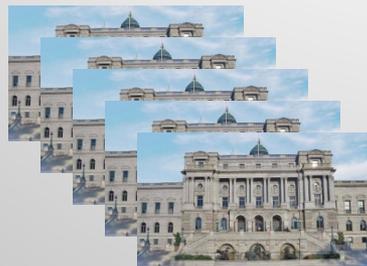
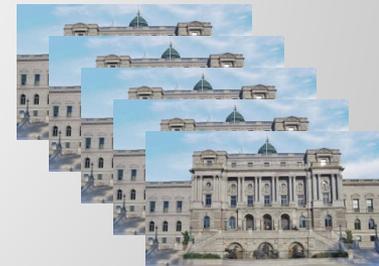
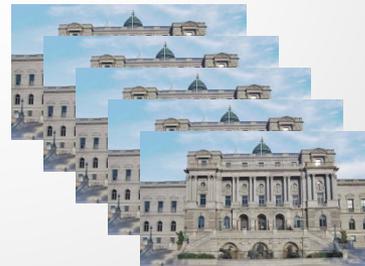
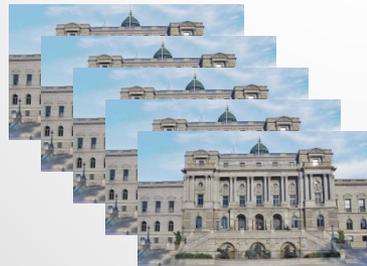
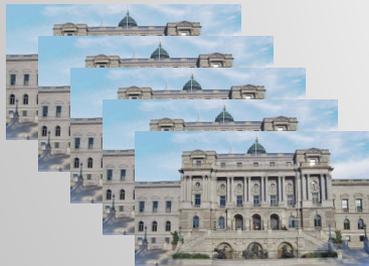
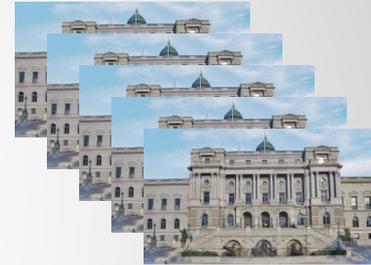


1 Terabyte of Data



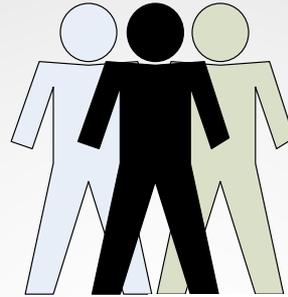
1 Large Library

A Typical Public Facing IT System Can Contain Over  
**35 Terabytes of Data**



# Anatomy of a Privacy Incident

## Breach of PII of 13,000 Individuals



EMAILED EXTERNALLY

CREATED  
SPREADSHEET FROM  
OFFICIAL RECORDS

SHARED  
INFORMATION

FAILED TO INTEGRATE  
PRIVACY AS PART OF  
THE MISSION

UNENCRYPTED  
TO OUTSIDE DHS

PERSON  
WITHOUT NEED  
TO KNOW

LACK OF PRIVACY  
AWARENESS

UNAUTHORIZED  
COPY OF SYSTEM  
OF RECORD OF  
13,000  
INDIVIDUALS

PRIVACY PROTECTION FAILURES



Case Comparison Worksheet

Case #	Case Name	Case Type	Case Status	Case Date
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

Existence of LI/Tenant Relationship: F or N  
Mapping Variables: F or N  
Sanctions: F or N  
Ownership: F or N  
Disposal: F or N  
Transfer to: F or N



**Assess Privacy Risks By Type of Work Environment**

# Maintain a Privacy Inventory



# Manage Your Privacy Papers



# Manage Your Privacy Electrons





NATIONAL ARCHIVES

Research Our Records | Veterans Service Records | Teachers' Resources

### Guide to Federal Records

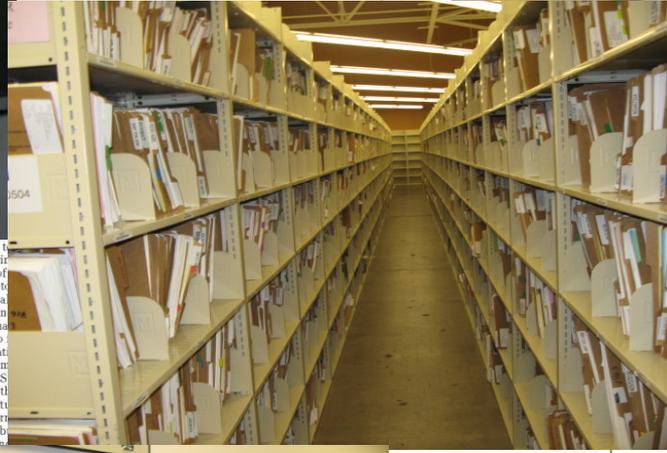
Home > Research Our Records > Guide to Federal Records > Records of the United States Coast Guard

**Records of the United States Coast Guard (Record Group 26) 1785-1988**

**Overview of Records Locations**

**Table of Contents**

- 26.1 Administrative History
- 26.2 Records of the Bureau of Lighthouses and Light Stations
  - 26.2.1 General records
  - 26.2.2 Records relating to operations
  - 26.2.3 Personnel and payroll records
  - 26.2.4 Accounting records
  - 26.2.5 Records of lighthouse districts
  - 26.2.6 Records of collectors of customs and excise
- 26.3 Records of the Revenue Cutter Service and Revenue Marine
  - 26.3.1 General records
  - 26.3.2 Records relating to operations



**AGENCY XYZ**  
DISPOSITION REFERENCE GUIDE FOR MOST COMMON RECORDS

Record	Dispose of After	Authority
Public Officer Records	6 years & 3 months	GRS-6a
Product Inspection	5 years old	IM-14
Departure Documents	After data entry	NCI-85-83-7/1e
Investigations	15 years after closing	N1-36-92-1
Declarations – Dutiable	Attach to Collection Package	GRS-6
Declarations–Free	6 months	N1-36-98-1
Imports	5 years	GRS-5
Collection Packages	6 years & 3 months	GRS-6
Imports, originals at NPC*	See GRS-3 for dollar value	GRS-3
Imports – Executive	5 years	GRS-5
Imports – Not Executive	3 years	GRS-5
Imports, purchase less than \$2,000	2 years	GRS-5

**DEPARTMENT OF HOMELAND SECURITY**

Office of the Secretary  
(Docket No. DHS-2011-0003)

Privacy Act of 1974: Department of Homeland Security Office of Operations Coordination and Planning—004 Publicly Available Social Media Monitoring and Situational Awareness Initiative System of Records

AGENCY: Privacy Office, DHS.  
ACTION: Notice of Privacy Act system of records.

**SUMMARY:** In accordance with the Privacy Act of 1974, the Department of

DHS is issuing a specific SORN for this activity. This newly established system will be included in the Department of Homeland Security's inventory of record systems.

**DATES:** Submit comments on or before March 3, 2011. This new system will be effective March 3, 2011.

**ADDRESSES:** You may submit comments, identified by docket number DHS-2011-0003 by one of the following methods:

- **Federal e-Rulemaking Portal:** <http://www.regulations.gov>. Follow the instructions for submitting comments.
- **Fax:** 703-483-2999.
- **Mail:** Mary Ellen Callahan, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

law defines the "transparency" or "awareness" as "information from a variety of sources communicated to and decision making." OPS has this Initiative to provide situational awareness to establish a common platform in doing so, OPS components will achieve this status collection is currently DHS/OPS-003 to more transparently specific SORN. The NOC platforms that follow act publicly available

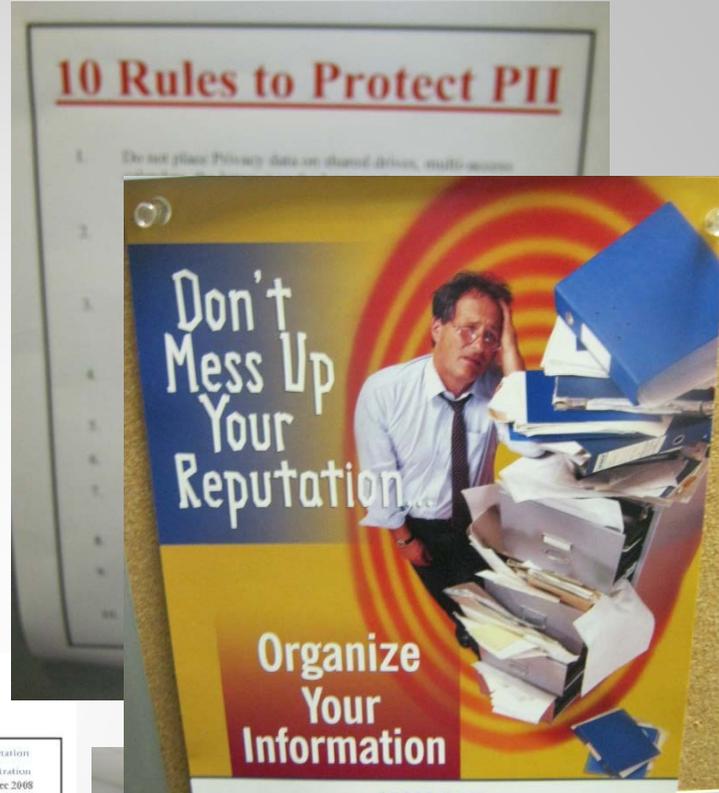


# Implement Sound Records Management



Hold Contractors Accountable

# Develop Privacy Champions



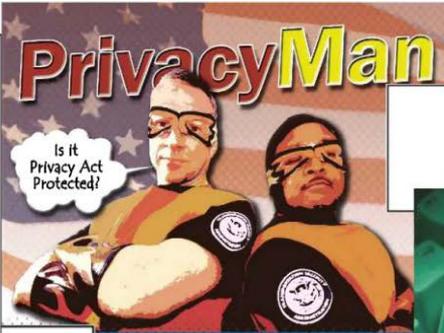
**PII/PIA Checklist**

**Privacy Analysis Worksheet**

System Name: \_\_\_\_\_

The Privacy Impact Assessment (PIA) determines what kind of personally identifiable information (PII) is contained within a system, what is done with that information, and how that information is protected. Systems with PII are subject to an extensive list of requirements based on privacy laws, regulations, and guidance.

- SEE LEFT OUT
- NOT LOCKING COMPUTER BEFORE LEAVING THE DESK
- NOT FOLLOWING CLEANDESK POLICY
- FOUND PAPER BY TRASH



**TRANSPORTATION SECURITY ADMINISTRATION**  
Dec 2008

**PRIVACY AWARENESS PRESS**

**TSA Broadcast**  
Thursday, December 11, 2008 1:42 PM  
3700 S - Updated Management Directive on Handling Sensitive Personally Identifiable Information

From: \_\_\_\_\_  
Sent: \_\_\_\_\_  
Subject: \_\_\_\_\_

Date: Dec. 11, 2008

**Extra Extra! Privacy Trivia**

The first individual to submit the correct (b) programs created by Dr. S answers to questions 1-4 wins a special Faikien prize and designation as Honorary (c) remote terminals Privacy Guru! (d) PayPal

**Secure Flight's Privacy Initiatives**

The Secure Flight Team will be calling on every single member of the Secure Flight Team to

**FEDERAL SECURITY DIRECTOR OFFICE INSPECTION PROGRAM**  
**INSPECTION CHECKLIST**  
**OPERATIONS**

Period of Review: \_\_\_\_\_ Office: \_\_\_\_\_

**A. INCIDENT REPORTING / NOTIFICATION PROCEDURE**



# Continuously Monitor Your Privacy Ecosystem

A blurred background image of a beach. In the foreground, there is a sandcastle with a red flag on top. The background shows the ocean waves and a clear blue sky.

## Office of Inspector General:

Marj Leaming, Director (202) 254-4172 [marj.leaming@oig.dhs.gov](mailto:marj.leaming@oig.dhs.gov)

## Transportation Security Administration:

Peter Pietra, Privacy Officer (571) 227-3654 [peter.pietra@tsa.dhs.gov](mailto:peter.pietra@tsa.dhs.gov)



**WHO**

**WHAT**

**WHERE**

**WHEN**

**WHY**

**HOW**

**QUESTIONS**

**ANSWERS**