

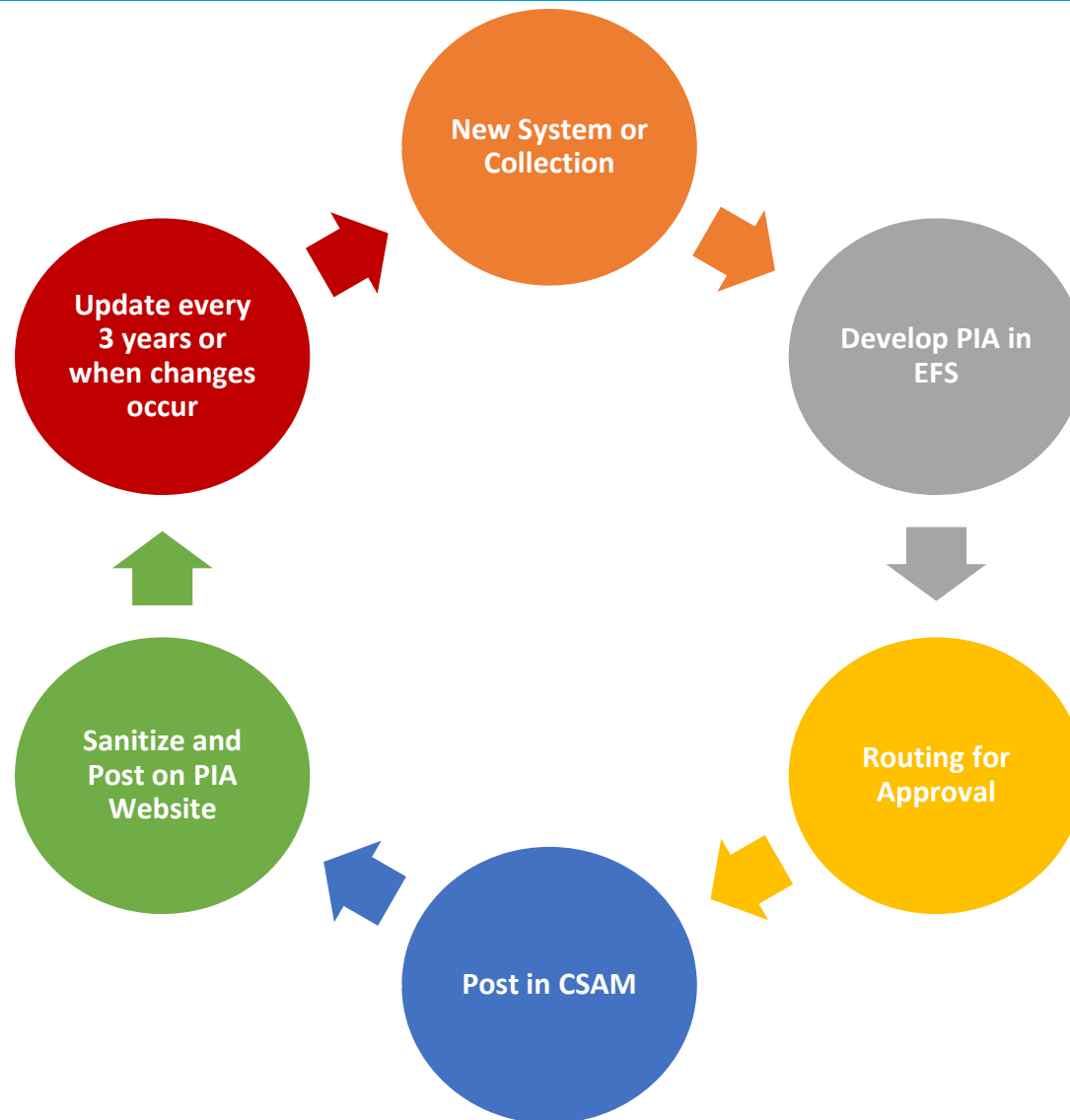


U.S. Department of the Interior
Office of the Chief Information Officer

Privacy Impact Assessments

Departmental Privacy Office

Lifecycle of a PIA



Privacy Impact Assessments (PIAs)

- Required by E-Government Act of 2002 and implemented by OMB M-03-22. Agencies must conduct PIAs when:
 - Developing or procuring any new technologies or systems that handle or collect PII.
 - Reviewing Information Collection Requests that gather PII including forms under the Paperwork Reduction Act.
 - Developing system changes that affect PII or create privacy risk.
- A PIA is an analysis of how information is handled and how PII is collected, used, maintained and disseminated.
- It is an important tool used to identify, evaluate and analyze potential privacy risks associated with the development or use of information systems or applications.
- Goals accomplished in completing a PIA include:
 - Making informed policy and system design or procurement decisions.
 - Accountability for privacy issues;
 - Analyzing both technical and legal compliance with applicable privacy laws and regulations, as well as accepted privacy policy; and
 - Providing documentation on the flow of personal information and information requirements within DOI systems.



DOI PIA Guide

- Issued September 30, 2014 and available on the DOI Privacy Program website.
- Provides detailed guidance on conducting PIAs to identify, evaluate and analyze potential privacy risks associated with the development or use of information systems or applications.
- All major and minor applications, general support systems, and sub-systems must be covered by a PIA that identifies and addresses privacy implications, regardless of whether the data is on members of the public or employees.
- Requires Bureaus and Offices to complete:
 - DI-4001 PIA form in the EFS when conducting assessments of any new or modified information systems
 - Adapted PIA for assessments of third-party websites and applications
- Incorporates NIST privacy controls and requires SAOP approval of the privacy controls implemented for an information system prior to issuance of an ATO.
- SAOP approval of privacy controls is documented through the PIA process.



PIA Development Process

- The PIA is a collaborative process and must address all aspects of the information lifecycle. The PIA is expected to be revised for different phases of this lifecycle, and should be reviewed at least every three years or upon any changes to the system/application or in privacy risk.
- PIAs should be started early during system planning, as it is more cost effective to build in adequate privacy protections and IT security than to retrofit later.
- The System Owner is responsible for initiating and completing the PIA with the Privacy Officer, and PIAs require collaboration with IT Security, Privacy Act System Manager, Records Management Officer, and Information Collection Clearance Officer.
- PIAs must be approved by the Reviewing Official - the DOI CIO/SAOP has delegated this responsibility to the Departmental Privacy Officer for Department-wide and OS PIAs. ADIRs are Reviewing Officials for bureaus.
- **New:** PIAs for systems requiring an ATO must be submitted to the Departmental Privacy Officer for approval. Follow the bureau process, however, the Bureau Privacy Officer will submit to Departmental Privacy Officer.




DI-4001 PIA Form

- The DI-4001 PIA form is an automated form with electronic signature capability.
- Mandatory for all PIAs conducted on systems at DOI.
- Available to all DOI personnel on the Enterprise Forms System (EFS) portal at <https://eforms.doi.gov>, the Department's enterprise-wide forms system.

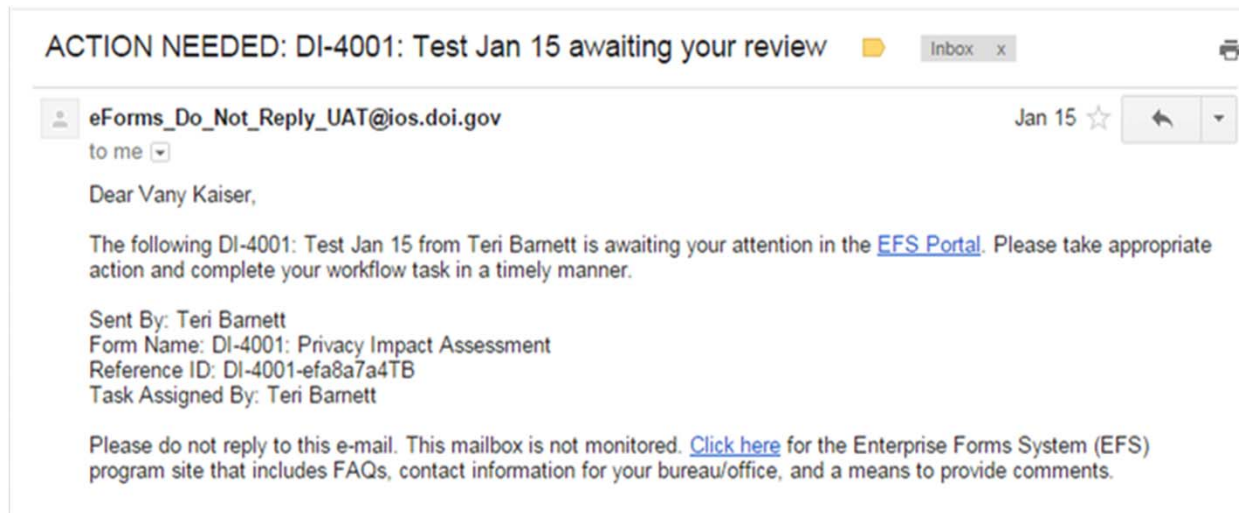


Tips for Completing the DI-4001 PIA Form

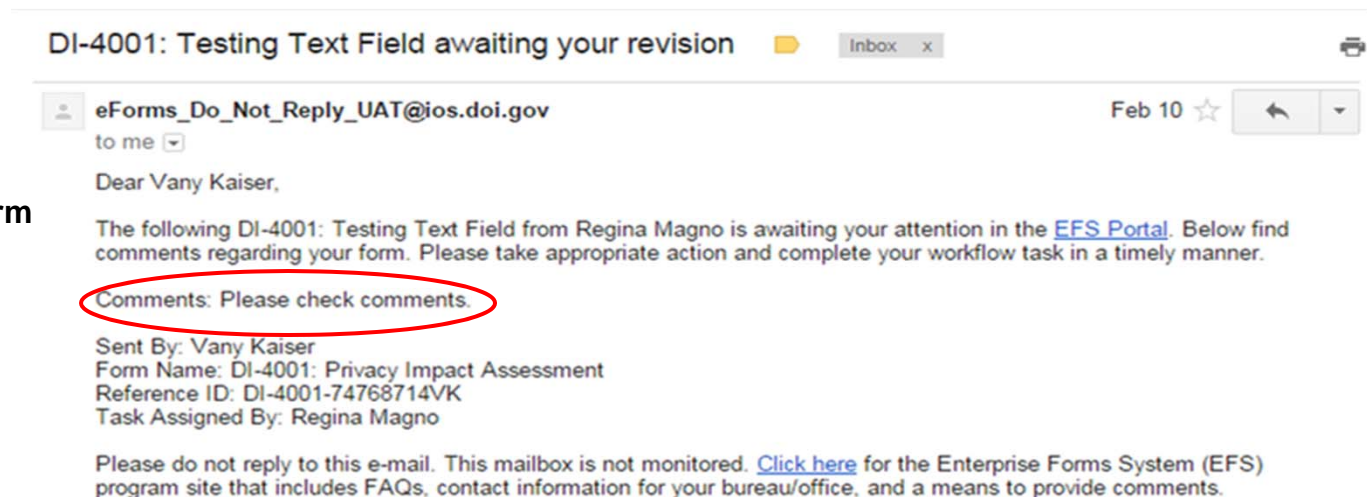
- A System Owner or Preparer can start a form, and can click on the Help buttons  for additional guidance for each question.
- Address appropriate privacy controls for each question, and provide explanation in the text fields when necessary.
- No character limits for text fields. Use complete and grammatically correct sentences. Remember that PIAs are published for public viewing - forms will be returned if incorrect or incomplete.
- Spell check feature is available - please use it.
- Do not include actual PII or any sensitive or proprietary information.
- The final PDF receipt has electronic signatures of all approving officials, and will be disseminated via email to all approvers after the Reviewing Official signs the form.
- Recommend collaboration before starting the form in EFS.
- Word version of PIA form in Appendix A of the Guide is located in the [DOI PIA Guide](#) folder in the DOI Privacy Portal.



Examples of EFS Email Notifications



Notification for Approving Official



Notification for Returned Form



Guidelines for Drafting a PIA

PIAs should be clear, unambiguous, and understandable to the general public. Any system or new collection that processes PII should be able to demonstrate that an in-depth analysis was conducted to ensure that privacy protections were built into the system.

- **Use Plain English.** Use words or phrases that are readily known to the average person.
- **Be detailed.** The PIA should be written with sufficient detail to permit the Privacy Office to analyze the privacy risks and mitigation steps.
- **Be consistent.**
- **Answer all questions.** If a particular question is not applicable please explain why it is not applicable, do not merely state “Not Applicable” – this will cause the PIA to be returned for further clarification.
- **Correct simple errors.** PIAs should be free of spelling and grammatical errors and written in active voice rather than passive voice.
- **Explain Acronyms.** Spell out each acronym the first time it is used in the document.
- **Define technical terms or references.**
- **Cite legal references and other previously published documents.**



Contents of a PIA

- **Introduction** - Name of the system or project, and bureau or office contact information.
 - **Section 1: General System Information** - Describes the purpose, legal authorities, and contains a threshold question to determine if the system collects, maintains, uses or disseminates information about individuals.
 - **Section 2: Summary of System Data** - Describes the specific PII in the system, the intended uses of the PII, with whom it will be shared, and how individuals can consent or decline to provide it.
 - **Section 3: Attributes of System Data** - Describes how the data will be verified for completeness and currency, how the data is handled, and the records management requirements.
 - **Section 4: PIA Risk Review** - Describes the privacy risks, and the physical, technical and administrative controls implemented.
 - **Section 5: Review and Approval** - Signatures of Approving Officials.
-



PIA Form developed in EFS: “Exercise: Consolidated Financial System”



Tips for Completing Introduction Section

- The point of contact should be someone that can respond to questions about the system and the PIA, this is generally the Privacy Officer. This individual's contact information is included in the published PIA on the DOI PIA website for public viewing.
- Employees must access the EFS Portal at least once to activate their account.
- If an individual is not registered in the EFS, the following error message appears when entering the individual's email address in the form: "The email address you have entered does not currently exist in the Enterprise Forms System (EFS). Please contact the recipient to confirm they have completed their EFS site registration."
- **Ensure Approving Officials access the EFS Portal at least once to activate their EFS account** - or you may not be able to route the form to them in EFS.



Tips for Completing Section 1, General System Information

Threshold question to determine if the system collects, maintains, uses or disseminates information about individuals.

- **Question A, Is a PIA required?** If “No” is selected, only Sections 1 and 5 need to be completed. The entire PIA must be completed for systems that contain information identifiable to individuals - also known as PII - including employees, contractors and volunteers.
- **Question E, Is this information system registered in CSAM?** Enter the Unique Investment Identifier (UII) Code found in the Cyber Security Assessment and Management (CSAM) system.
- **Question F, List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.** All subsystems must be listed - this information is verified against CSAM records and the PIA will be returned if not complete. Enter “Not applicable” if there are no minor applications or subsystems hosted on the system.



Tips for Completing Section 2, Summary of System Data

Describes the PII in the system.

- **Question A, What PII will be collected?** Be sure to indicate all the types of PII collected or maintained in the system. Responses for Privacy Act systems will be verified with the published SORN.
- **Question D, What is the intended use of the PII collected?** The intended use must be relevant to the purpose of the system. For Privacy Act systems, uses must be consistent with published SORNs.
- **Question E, With whom will the PII be shared, both within DOI and outside DOI?** If there is a sharing agreement, MOU, or Computer Matching Agreement, provide an explanation. For Privacy Act systems, describe how an accounting for disclosures is maintained.
- **Question G, What information is provided to an individual when asked to provide PII data?** If possible, a copy of the Privacy Act Statement, Privacy Notice, or a link to the applicable privacy policy, procedure, PIA or referenced SORN should be provided for review.
- **Question H, How will data be retrieved?** A complete response is important as it helps identify whether it is a Privacy Act system of records.



Tips for Completing Section 3, Attributes of System Data

Describes how the data will be verified and checked for completeness; how data will be handled; and the records requirements.

- **Question D, What are the retention periods for data in the system?**
Bureau/Office Records Officers should be consulted early in the development process for records requirements. Include records retention schedules for different types of information or subsets of information.
- **Question E, What are the procedures for disposition of the data at the end of the retention period?** This information may be obtained from records retention schedules, the Departmental Manual, bureau/office records management policies, or standard operating procedures.
- **Question F, Briefly describe privacy risks and how information handling practices at each stage of the “information lifecycle” affect individual privacy.** It is important to provide sufficient detail in the explanation for how PII is handled at each stage of the record to allow adequate review and assessment.



Tips for Completing Section 4, PIA Risk Review

Describes the privacy risks for this system.

- **Question G, Who will have access to data in the system or electronic collection?** Include all users who access or view the data - system owners and managers, system administrators, end users, etc.
- **Question I, Are contractors involved with the design and/or development of the system...?** Contractors are subject to the same privacy requirements as federal employees. Contracts must include Privacy Act clauses and other privacy and security provisions.
- **Question M, What controls will be used to prevent unauthorized monitoring?** For example, business rules, internal instructions, access controls, least privileges, audit features or logs, posting DOI Privacy Act Warning Notices.
- **Question N, How will the PII be secured?** It is important to identify **all** applicable physical, technical, and administrative controls. If controls implemented for the system are not listed, choose “Other” and provide an explanation.



Tips for Completing Section 5, Review and Approval

PIAs must be approved by


- *Information System Owner*
 - *Information System Security Officer*
 - *Privacy Officer*
 - *Reviewing Official*
-
- Privacy Officer and Reviewing Official can return a form for revision with comments.
 - Forms are returned to the System Owner or Preparer - the individual that started the form - to revise and resubmit.
 - After the Reviewing Official signs the form, all approving officials will receive an email notification with a pdf copy of the form.

Information System Owner

Email
Vany_Kaiser@ios.doi.gov

First Name M.I. Last Name Title
Vany Kaiser Departmental Privacy Act Specialist

Bureau/Agency Phone
Office of the Chief Information Officer (202) 208-3387


 Electronically signed by: Vany Kaiser
Date: Mon Mar 02 2015 13:27:41 GMT-0500
Reference number: DI-4001-d59eed0bVK
U.S. Department of the Interior | Enterprise Forms System

Information System Security Officer

Email
Christopher_Rutherford@ios.doi.gov

First Name M.I. Last Name Title
Christopher Rutherford DCISO

Bureau/Agency Phone
Office of the Chief Information Officer (202) 208-5433


 Electronically signed by: Christopher Rutherford
Date: Mon Mar 02 2015 13:43:29 GMT-0500
Reference number: DI-4001-d59eed0bVK
U.S. Department of the Interior | Enterprise Forms System

Privacy Officer

Email
Regina_Magno@ios.doi.gov

First Name M.I. Last Name Title
Regina Magno Privacy Act Specialist

Bureau/Agency Phone
Office of the Chief Information Officer (303) 969-5513


 Electronically signed by: Regina Magno
Date: Mon Mar 02 2015 11:48:46 GMT-0700
Reference number: DI-4001-d59eed0bVK
U.S. Department of the Interior | Enterprise Forms System

Reviewing Official

Email
teri_barnett@ios.doi.gov

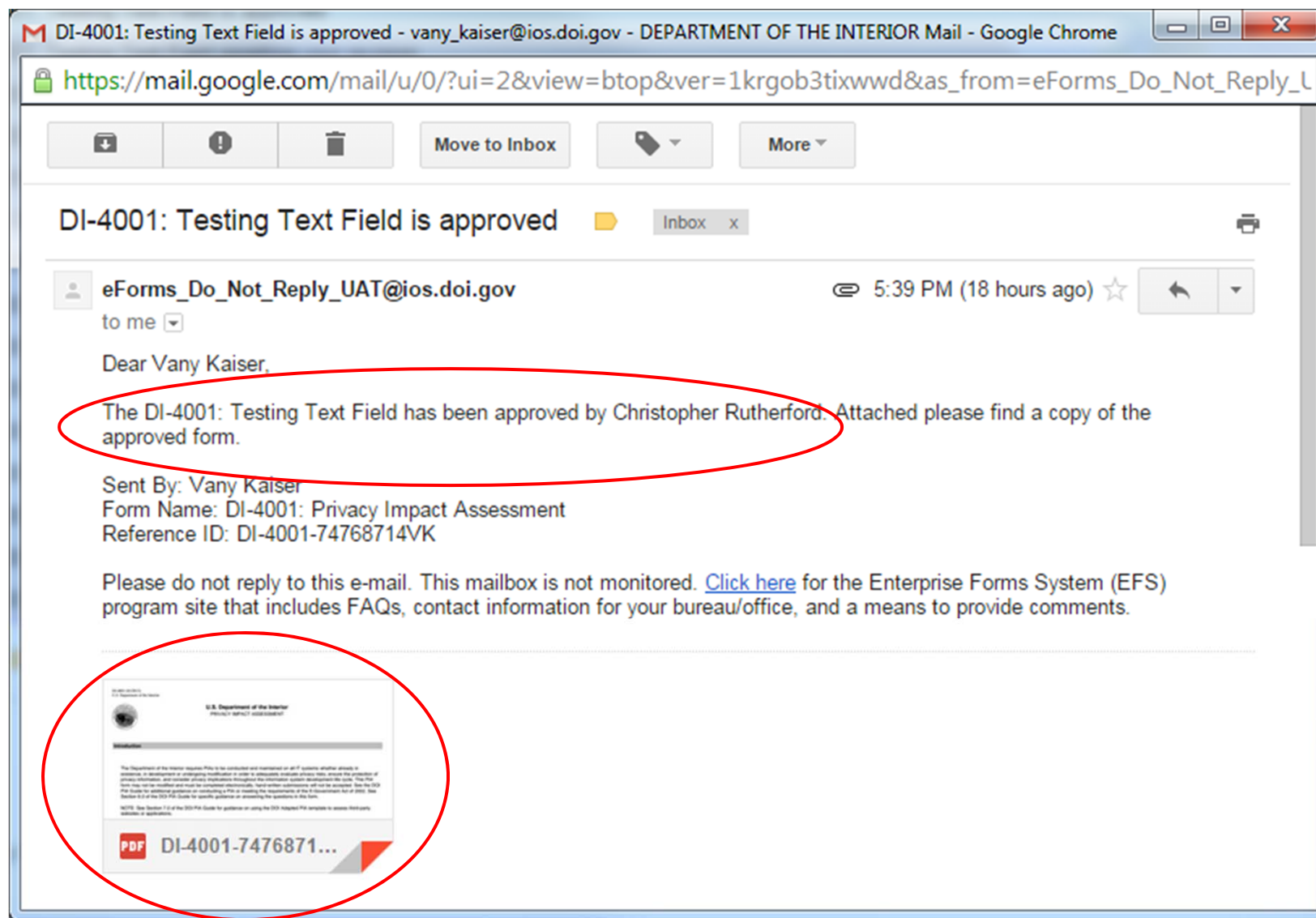
First Name M.I. Last Name Title
Teri Barnett DPO

Bureau/Agency Phone
Office of the Chief Information Officer (202) 208-1943

 Electronically signed by: Teri Barnett
Date: Mon Mar 02 2015 15:51:19 GMT-0500
Reference number: DI-4001-d59eed0bVK
U.S. Department of the Interior | Enterprise Forms System



Email Notification for Approved Form



Roles for PIA Approval

All PIAs conducted must contain Reviewing Official signatures to indicate privacy implications are adequately identified, evaluated and addressed.

- **Information System Owner** - Official with overall responsibility for the operation or maintenance of an information system and compliance with legal and policy requirements. This official is identified in CSAM.
- **Information System Security Officer** - This official is designated by the System Owner for the information system and is generally identified in CSAM. A Bureau Chief Information Security Officer may also approve PIAs and Adapted PIAs for third-party websites and applications.
- **Privacy Officer** - Privacy Officer reviews PIAs to ensure privacy implications are addressed and adequate privacy controls are implemented.
- **Reviewing Official** - The Departmental Privacy Officer has delegated authority as the Reviewing Official to approve Department-wide and OS PIAs, and PIAs for information systems requiring an Authority to Operate (ATO). Bureau and Office ADIRs are Reviewing Officials on PIAs for systems developed and maintained by a Bureau or Office.



Posting PIAs in CSAM

- The Cyber Security Assessment and Management (CSAM) system is the Department's official repository of information systems.
 - Completed PIAs must be posted for each system entry in CSAM. Bureau employee access to CSAM is based on roles and may be limited by the bureau.
1. <https://csam.doi.net/CSAM/>
 2. Login in with username and password
 3. Click on "Accept"
 4. Click on "System" then select "Search Systems" under the System drop-down menu.
 5. Enter system name or acronym or select bureau/office.
 6. Click on Search button.
 7. Select "Details" for the system.
 8. In System Overview, select "Status & Archive".
 9. In the Privacy section, click on the number in the Privacy Impact Assessment row.
 10. Click on "+ Add New Artifact".
 11. Click on "Search for and attach existing Artifact" tab or "Add New Artifact" tab.



Screenshots of Privacy Section in CSAM

Privacy				
	Status		Date Completed	Artifacts
Privacy Threshold Analysis			4/1/2013	0
Personally Identifiable Information	Yes			
Privacy Impact Assessment	Required under E-Government Act		4/1/2013	1
System of Records Notice	Required under Privacy Act			2
Edit				

Privacy Section in CSAM

Click on the number under the Artifacts column to view or upload a new PIA.

Pop up Window to upload a new PIA.

CSAM Popup

Search for and attach existing Artifact

Add New Artifact

Select the file(s) then click 'Upload'. Additional files can be selected by clicking the 'Add' button. A description is required for all files uploaded.

Description

File

Select

Remove

Add

Upload

Cancel Add

Limited Official Use

Adapted PIA for Third-Party Websites and Applications

- OMB M-10-23, Guidance for Agency Use of Third Party Websites and Applications, requires agencies to take steps to protect privacy when using social media websites including:
 - Examining existing third-party privacy policies for adequacy
 - Posting Privacy Notices on third-party websites to inform the public that the application is operated by a third-party, the agency's Privacy Policy does not apply requirements
 - Using Pop-ups for external links to third-party sites alerting the viewer that they are leaving a Government website
 - Disclosing any embedded applications and uses in the DOI Privacy Policy
 - Providing agency branding
 - Minimizing the collection of information needed to accomplish the agency's function
 - OMB Memorandum, Model Privacy Impact Assessment for Agency Use of Third-Party Websites and Applications - An Adapted PIA is required whenever an agency's use of a third-party website or application makes PII available to the agency so organizations can take steps to assess the inherent risks associated with use of third-party websites and applications before engaging the public.
 - DOI Adapted PIA Word template is available on the DOI Privacy Portal. See the DOI PIA Guide Appendix B for guidance on completing an Adapted PIA.
-

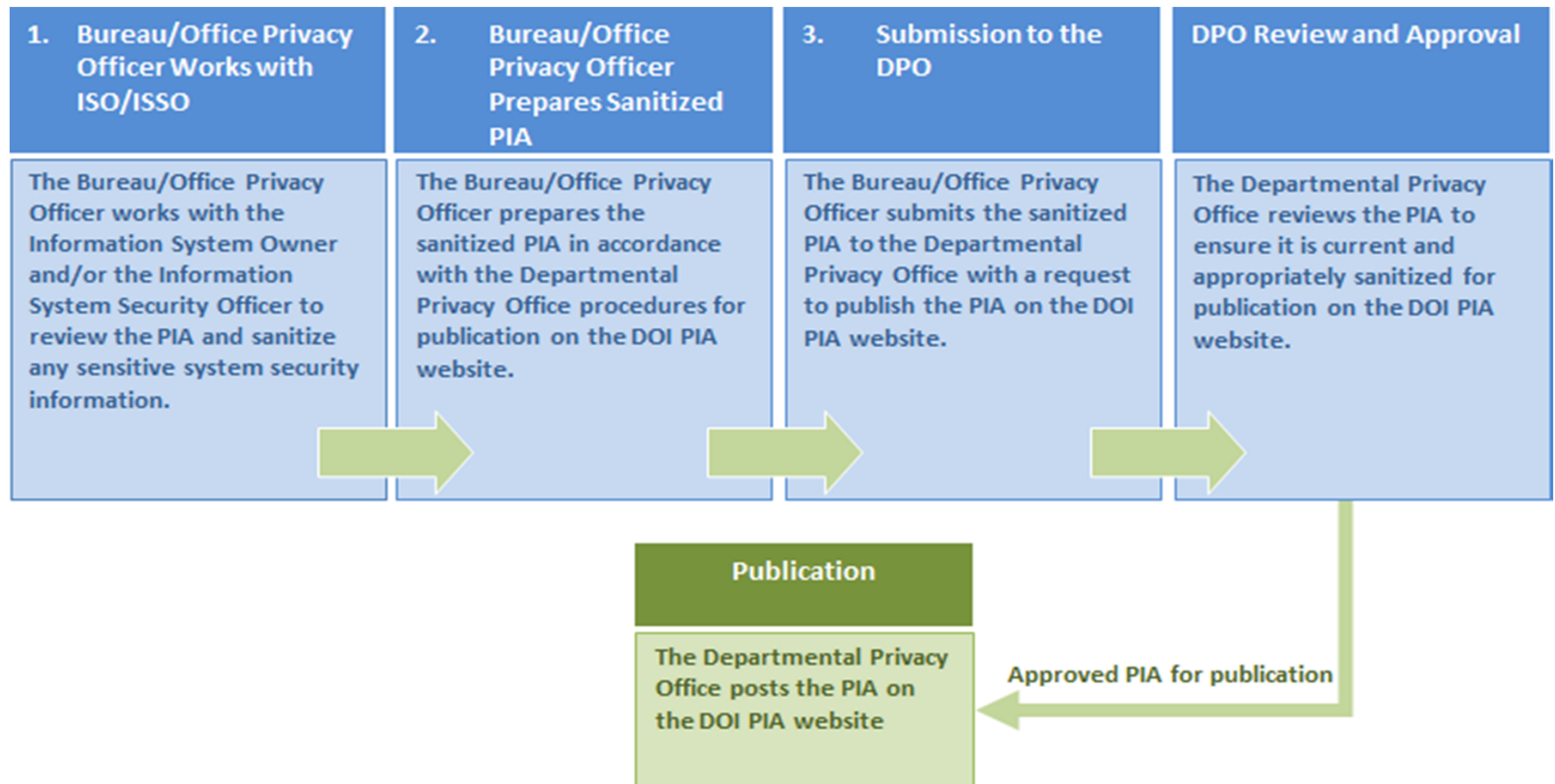


Adapted PIAs

- Each Adapted PIA should be tailored to address the specific functions.
 - One Adapted PIA may be conducted to cover multiple websites or applications as long as the agency's practices are substantially similar across each website and application. However, any use of a third-party website or application that raises distinct privacy risks requires an Adapted PIA specifically for the website or application that includes a tailored analysis of that use.
 - The requirements of the Privacy Act apply to information collected, used, or made available using a third-party website or social media application.
 - Program officials must work with Bureau Privacy Officers to complete an Adapted PIA to ensure privacy risks are identified and addressed, and that Privacy Act and other legal requirements are met, and may need to coordinate certain responses with Bureau Information Collection Clearance Officer, Records Officer, and Information Security Officer.
 - Department-wide Adapted PIAs are approved by the Departmental Privacy Officer as the Reviewing Official. Bureau level Adapted PIAs are approved by the Bureau ADIR as the Reviewing Official.
 - Adapted PIAs are posted to the DOI PIA website for public viewing.
-



Steps for Publishing a PIA



Sanitizing and Publishing PIAs

- Bureau/Office PIAs must be submitted in the approved sanitized format with any sensitive system information redacted, and for older PIAs the signature page must be removed before it can be made available to the public.
- PIAs should not contain PII or any information related to employees that might be used to blackmail, compromise or otherwise influence a DOI employee's ability to perform the duties of their position. These information types may present a risk to the security of the DOI network, information assets, or organizational operations (including mission, functions, or organizational assets).
- Below are examples of information types that should NOT be released
 - Information describing networks or network connectivity (IP addresses, network diagrams, discussions detailing the type of network equipment used or details regarding the types of network connectivity used in the network)
 - Information describing the hardware, software or configuration details of a system or computer devices in the system
 - Explanations on how information flows to or from a system (flow charts, written flow descriptions, etc.)
 - Contact information for DOI employees that links to their technical roles or responsibilities in the environment
 - User account and password or PIN information for any DOI employee
 - Any information about law enforcement or national security systems managed by DOI



Privacy Quiz

When should a PIA be reviewed and updated?

- A. Every year.
- B. Every three years.
- C. When there is a change in the system configuration that implicates privacy.
- D. When there is a change in how PII is collected and processed.

Bonus: Who is responsible for updating a PIA? **System Owner**



Privacy Quiz

Who is the Reviewing Official that approves PIAs?

- A. System Owner
- B. Chief of Staff
- C. Chief Information Security Officer
- D. ADIR**
- E. Departmental Privacy Officer**



Privacy Quiz

You are the Bureau Privacy Officer. Your Bureau Web Manager and a Program Official contact you because they would like to use Facebook to promote their program and facilitate communication and outreach to the public.

What is your next step?

- A. No way - that is too risky.
- B. Refer them to the CSAM point of contact.
- C. Provide guidance on how to use the DI-4001 PIA form in EFS.
- D. Provide the DOI PIA Guide and the DOI Adapted PIA template to start the assessment of the agency's official use of the third-party social media application.**



Privacy Resources

- Privacy Act of 1974 <http://www.justice.gov/opcl/privstat.htm>
- E-Government Act of 2002 <http://thomas.loc.gov/cgi-bin/query/F?c107:1:./temp/~c107aSi1Tc:e72517>
- Federal Information Security Management Act (FISMA) <http://csrc.nist.gov/drivers/documents/FISMA-final.pdf>
- Intelligence Reform and Terrorism Prevention Act of 2004 <https://it.ojp.gov/default.aspx?area=privacy&page=1282>
- Freedom of Information Act, as amended (FOIA) <http://www.justice.gov/oip/amended-foia-redlined-2010.pdf>
- Paperwork Reduction Act <http://www.archives.gov/federal-register/laws/paperwork-reduction/>
- Clinger-Cohen Act http://www.cio.gov/Documents/it_management_reform_act_feb_1996.html
- OMB Privacy Guidance http://www.whitehouse.gov/omb/privacy_default
- DOI Privacy Program Website <http://www.doi.gov/ocio/privacy/>
- 383 Departmental Manual Chapters 1-13 http://elips.doi.gov/app_dm/dm.cfm
- DOI Privacy Act Regulations, 43 CFR Part 2, Subpart K <http://www.doi.gov/foia/43cfrsub.html>
- DOI Privacy Intranet http://www.mydoi.doi.net/ocio/imd/ocio_privacy.html
- DOI Privacy Portal <https://portal.doi.net/CIO/IAD/ORG/privacy/default.aspx>



Privacy Office Contacts

Departmental Privacy Office:

Teri Barnett, Departmental Privacy Officer
202-208-1943, Teri_Barnett@ios.doi.gov

Vany Kaiser, Privacy Act Specialist
202-208-3387, Vany_Kaiser@ios.doi.gov

Regina Magno, Privacy Act Specialist
303-969-5513, Regina_Magno@ios.doi.gov

Bureau Privacy Officers: <http://www.doi.gov/privacy/contacts>



Questions?



U.S. Department of the Interior
Office of the Chief Information Officer