

**U.S. Department of Commerce
Office of the Secretary**



**Privacy Threshold Analysis for the
Freedom of Information Act Online Tracking System (FOIAonline)**

U.S. Department of Commerce Privacy Threshold Analysis
Office of the Secretary
Freedom of Information Act Online Tracking System (FOIAonline)

Unique Project Identifier: EPA FOIAonline

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description of the information system in a way that a non-technical person can understand.*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition. "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)

The FOIAonline system is an electronic tracking and processing tool developed as a partnership of Federal agencies that allows anyone to submit a Freedom of Information Act (FOIA) request, correspond with FOIA professionals processing the request, track the status of a request, and download any documents responsive to a request after they are released to the requester. The FOIAonline system is used by Department of Commerce (DOC) bureaus and operating units (except for the U.S. Patent and Trademark Office) and other Federal agencies, such as the Environmental Protection Agency, the Department of the Navy, and the Small Business Administration. The system enables agencies to publish FOIA documents in electronic format with responses, yielding cost savings by eliminating duplicate work. Communications between agencies can be done online, reducing costs and speeding up response times to requesters. The system provides participating agencies with a records management system, and the ability to collect FOIA metrics and generate mandatory Department of Justice FOIA reports. The system responds to the President's and Attorney General's commitment to accountability and transparency by taking "affirmative steps to make information public," and applying "modern technology to inform citizens about what is known and done by their Government."

Records are obtained from those individuals who submit requests and administrative appeals pursuant to the FOIA and the Privacy Act of 1974, as amended, or who file litigation regarding such requests and appeals; the agency record keeping systems searched in the process of responding to such requests and appeals; Departmental personnel assigned to handle such requests, appeals, and/or litigation; other agencies or entities that have referred to DOC requests concerning DOC records, or that have consulted with DOC regarding handling of particular requests; and submitters or subjects of records or information that have provided assistance to DOC in making access or amendment determinations.

A typical FOIA/Privacy Act (PA) transaction includes the requester's name, home or business address, personal or business email address, home or business telephone number, and a description of the requested records. FOIA requests are logged in to the system and assigned a case number for the purpose of identifying and tracking the processing of the request and for statistical reporting requirements. Information sharing is on a case-by-case, with a need to know basis within the agency.

The information is collected, maintained, used, and disseminated in accordance with 5 U.S.C. 552; 44 U.S.C. § 301; 5 U.S.C. § 301; and 5 U.S.C. 552a.

Questionnaire:**1. What is the status of this information system?**

- This is a new information system. *Continue to answer questions and complete certification.*
- This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)			
a. Conversions		d. Significant Merging	g. New Interagency Uses
b. Anonymous to Non-Anonymous		e. New Public Access	h. Internal Flow or Collection
c. Significant System Management Changes		f. Commercial Sources	i. Alteration in Character of Data
j. Other changes that create new privacy risks (specify):			

- This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*
- This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

Yes. *Please describe the activities which may raise privacy concerns.*

No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential" (5 U.S.C. 552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)"

Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

- Companies
- Other business entities

No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

- DOC employees
- Contractors working on behalf of DOC
- Members of the public

No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc

- Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.
- No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

X I certify the criteria implied by one or more of the questions above **apply** to the FOIAonline and as a consequence of this applicability, I will perform and document a PIA for this IT system.

 I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO):

Carrie Hyde-Michaels

Signature of ISSO: CARRIE HYDE-MICHAELS Digitally signed by CARRIE HYDE-MICHAELS
Date: 2019.04.02 16:59:03 -04'00' Date: _____

Name of Information Technology Security Officer (ITSO): Jun Kim

Signature of ITSO: JUN KIM Digitally signed by JUN KIM
DN: cn=JUN KIM, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, email=jun.kim@doe.gov, c=US Date: _____

Name of Authorizing Official (AO): Lisa Casias

Signature of AO: *Lisa Casias* Date: 4/24/19

Name of Bureau Chief Privacy Officer (BCPO): Wesley Fravel

Signature of BCPO: WESLEY FRAVEL Digitally signed by WESLEY FRAVEL
Date: 2019.04.16 16:57:48 -04'00' Date: _____