

**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 on 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 to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

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).

FOIAonline is a multi-agency web-application that enables the public to submit FOIA requests to participating agencies, track the progress of the agency’s response to request, search for information previously made available, and generate up-to-the minute reports on FOIA processing. FOIAonline is a workflow system and repository that enables partner agencies to receive, manage, track, and respond to FOIA requests, generate reports including the annual FOIA report that is submitted to the Department of Justice, communicate with requestors, and manage their FOIA case files as electronic records.

- a) *Whether it is a general support system, major application, or other type of system*
Major Application
- b) *System location*
System data is stored and maintained in the FedRAMP approved Amazon Cloud.
- c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*
FOIAonline is a stand-alone system and does not interconnect with systems outside of its boundaries.
- d) *The purpose that the system is designed to serve*

FOIAonline is designed to provide a multi-agency web-application that enables the public to submit FOIA requests to participating agencies, track the progress of the agency's response to request, search for information previously made available, and generate up-to-the minute reports on FOIA processing. FOIAonline is a workflow system and repository that enables partner agencies to receive, manage, track, and respond to FOIA requests, generate reports including the annual FOIA report that is submitted to the Department of Justice, communicate with requestors, and manage their FOIA case files as electronic records.

e) The way the system operates to achieve the purpose

FOIAonline is designed to provide a multi-agency web-application that enables the public to submit FOIA requests to participating agencies, track the progress of the agency's response to request, search for information previously made available, and generate up-to-the minute reports on FOIA processing. FOIAonline is a workflow system and repository that enables partner agencies to receive, manage, track, and respond to FOIA requests, generate reports including the annual FOIA report that is submitted to the Department of Justice, communicate with requestors, and manage their FOIA case files as electronic records.

f) A general description of the type of information collected, maintained, use, or disseminated by the system

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 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.

g) Identify individuals who have access to information on the system

All personnel have their status categorized with a sensitivity level in accordance with PS-2. Personnel (federal employees or contractors) of service providers are considered internal users. All other users are considered external users.

h) How information in the system is retrieved by the user

Users access data residing on their workstation or on network locations within the usual office automation applications (word processing, spreadsheet, database).

i) *How information is transmitted to and from the system*

Information can be copied from location to location if the user has appropriate access rights. Information can be sent via email if it is not sensitive. Information can be sent by a secure file transfer application if the data is sensitive.

Questionnaire:

1. Status of the Information System

1a. 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 01-2017). *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 01-2019 or later). *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

_____ Yes. This is a new information system.

_____ Yes. This is an existing information system for which an amended contract is needed.

☐ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

☒ No. This is not a new information system.

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. *(Check all that apply.)*

Activities			
Audio recordings	<input type="checkbox"/>	Building entry readers	<input type="checkbox"/>
Video surveillance	<input type="checkbox"/>	Electronic purchase transactions	<input type="checkbox"/>
Other (specify):			

☒ 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.

☒ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

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

- ☒ DOC employees
- ☒ Contractors working on behalf of DOC
- ☒ Other Federal Government personnel
- ☒ 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 Social Security numbers (SSNs), including truncated form?

☐ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
--

Provide the legal authority which permits the collection of SSNs, including truncated form.

☒ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. 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.

4d. 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, 4c, and/or 4d are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

☒ I certify the criteria implied by one or more of the questions above **apply** to the FOIAonline Tracking System 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 FOIAonline Tracking System and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

<p>Information System Security Officer or System Owner Name: Kenyetta Haywood Office: OPOG Phone: 202.482.3743 Email: khaywood1@doc.gov</p> <p>Signature: <u>KENYETTA HAYWOOD</u> Digitally signed by KENYETTA HAYWOOD Date: 2021.08.26 18:27:42 -04'00'</p> <p>Date signed: _____</p>	<p>Information Technology Security Officer Name: Jerome Nash Office: OS/OESS Phone: 202.482.3186 Email: jnash@doc.gov</p> <p>Signature: <u>JEROME NASH</u> Digitally signed by JEROME NASH Date: 2021.08.31 11:31:46 -04'00'</p> <p>Date signed: _____</p>
<p>Privacy Act Officer Name: Tahira Murphy Office: OPOG Phone: 202.482.8075 Email: tmurphy2@doc.gov</p> <p>Signature: <u>TAHIRA MURPHY</u> Digitally signed by TAHIRA MURPHY Date: 2021.09.21 13:02:12 -04'00'</p> <p>Date signed: _____</p>	<p>Authorizing Official Name: Lawrence W. Anderson Office: Office of the Secretary Phone: 202.482.4444 Email: landerson@doc.gov</p> <p>Signature: <u>LAWRENCE ANDERSON</u> Digitally signed by LAWRENCE ANDERSON Date: 2021.09.01 14:42:10 -04'00'</p> <p>Date signed: _____</p>
<p>Bureau Chief Privacy Officer Name: Maria Dumas Office: OPOG Phone: 202.483.5153 Email: mdumas@doc.gov</p> <p>Signature: <u>MARIA STANTON DUMAS</u> Digitally signed by MARIA STANTON-DUMAS Date: 2021.09.21 17:07:14 -04'00'</p> <p>Date signed: _____</p>	