Template Version Number: 01-2020

U.S. Department of Commerce
Office of the Secretary

Privacy Impact Assessment
for the
Freedom of Information Act Online Tracking System (FOIAonline)

Reviewed by: Maria D. Dumas Bureau Chief Privacy Officer

☑ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Jennifer Goode 09/30/2021

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
Office of the Secretary/Freedom of Information Act Online Tracking System (FOIAonline)

Unique Project Identifier: EPA FOIAonline

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

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, an 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 way the system operates to achieve the purpose(s) identified in Section 4*
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) 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).

(f) 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.

(g) Any information sharing conducted by the system

Information is shared within OS, within DOC bureaus, other federal agencies through government agencies, and via the public and private sectors on a case-by-case basis by DOC personnel. All FOIA case information is shared with the following federal agencies:

a. Other Federal agencies that are users of the systems for referrals and consultations.
b. Appeal officials for FOIA case administrative appeals.
c. The Department of Justice for FOIA case litigation and reporting.

Information is also shared via direct access within OS, DOC bureaus, and the public directly under the circumstances of FOIA requests made 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 Department of Commerce (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.

Information shared with the public:

a. FOIA request tracking number
b. Request type (Request, Appeal, Record, or Referral)
c. Status of request (Submitted, Evaluation, Assignment, Processing, or Closed)
d. Requester's name (may not be shared if privacy concerns are involved)
e. Requester's organization (may not be shared if privacy concerns are involved)
f. Request submitted date
g. Request completion date
h. Description of request (may not be shared if privacy concerns are involved)
i. Records released

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

PII is collected in this system is pursuant to:

1. Freedom of Information Act, 5 U.S.C. 552.
2. Government Organization and Employees, Title 5, U.S.C.

3. Records management by agency heads, 44 U.S.C. §3101.
4. Departmental regulations, 5 U.S.C. §301.
5. Privacy Act of 1974 as amended, 5 U.S.C. 552a.

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

Moderate

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.
_____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

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.

__✓__ 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).
____ 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).

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport		k. Financial Transaction	
c. Employer ID		h. Alien Registration		l. Vehicle Identifier	
d. Employee ID		i. Credit Card		m. Medical Record	

e. File/Case ID	✓				
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	✓	h. Date of Birth		o. Financial Information	✓
b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address	✓	q. Military Service	
d. Gender		k. Telephone Number	✓	r. Criminal Record	
e. Age		l. Email Address	✓	s. Physical Characteristics	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation		e. Work Email Address	✓	i. Business Associates	
b. Job Title	✓	f. Salary		j. Proprietary or Business Information	
c. Work Address	✓	g. Work History		k. Procurement/contracting records	
d. Work Telephone Number	✓	h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs		j. Weight		o. Dental Profile	
p. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	✓	c. Date/Time of Access	✓	e. ID Files Accessed	✓
b. IP Address		f. Queries Run		f. Contents of Files	✓
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax	✓	Online	✓
Telephone		Email	✓		
Other (specify):					

Government Sources					
Within the Bureau	✓	Other DOC Bureaus	✓	Other Federal Agencies	✓
State, Local, Tribal	✓	Foreign			
Other (specify):					

Non-government Sources					
Public Organizations	✓	Private Sector	✓	Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

FOIAonline allows the public to request copies of existing records managed by DOC bureaus. All DOC privacy and data accuracy policies apply to records associated with these requests.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
✓	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

✓	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

✓	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters		To promote information sharing initiatives	
For litigation	✓	For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in

reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The PII data will be used to associate the FOIA and/or Privacy Act (FOIA/PA) requesters with information they are seeking under the FOIA/PA. The PII data will also be used to contact requesters, other federal agencies, and staff fulfilling requests for information, as well as by requesters following up on the status of their requests. The PII identified in Section 2.1 of this document is in reference to federal employees / contractors, members of the public and private entities.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

There is always the potential for insider threat. All DOC employees, including those that maintain this application, are required to take annual cybersecurity and privacy awareness training. Also, system training for new users is provided by the vendor. Rules of behavior guidelines are adhered to for user access. All communication flows are encrypted. System access is limited to authorized account holders.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	✓		✓
DOC bureaus	✓		✓
Federal agencies	✓		

State, local, tribal gov't agencies	✓		
Public	✓		✓
Private sector	✓		
Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
✓	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
✓	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public	✓	Government Employees	✓
Contractors	✓		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

✓	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
✓	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://foiaonline.gov/foiaonline/action/public/privacy.	
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

✓	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Individual users can choose not to include their PII before submitting their requests. However, if individuals decide not to provide the required information, their requests cannot be entered into the: system or processed, pursuant of Commerce's FOIA regulations, 15 CFR H 4.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

✓	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Requesters are required to provide a name and mailing address to make a FOIA request, which is a public request, pursuant to the Department of Commerce's FOIA regulations, 15 CFR 4.4. Requesters are consenting to use of their PII (i.e. identifying requestors for fulfilling customer requests and communicating with the requestors) upon agreement to submit the request. Individual users can choose not to include their PII, but their requests cannot be entered or processed into the system.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

✓	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: The system requires individuals to review their PII before they submit their requests for information. Individuals with FOIAonline user accounts can also update their user profiles in the system to make changes to their individual information, which includes PII.
	No, individuals do not have an	Specify why not:

	opportunity to review/update PII/BII pertaining to them.	

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
✓	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
✓	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
✓	Access to the PII/BII is restricted to authorized personnel only.
✓	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: All activity within the system is tracked by an automated audit log.
✓	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 2/6/2019 (ATO expires 10/31/2021) ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
✓	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
✓	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
✓	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
✓	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish DOC ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
✓	Other (specify): Staff with access to PII will be required to either sign or programmatically acknowledge the "Rules of Behavior" document that dictates Standards of Acceptable System Use and Account Approval. These standards apply to all users of Department of Commerce Information Technology (IT) resources and are intended to increase individual awareness and responsibility, and to ensure that all users utilize IT resources in an efficient, ethical, and lawful manner. Failure to abide by these rules may constitute grounds for termination of access privileges, administrative actions such as disciplinary actions, and or criminal prosecution, if warranted. All users must read and acknowledge these standards to receive access to Department of Commerce IT resources, including specific provisions outlined in the document.

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

FOIAonline implements required FISMA technical controls for a FIPS 199 Moderate level system and is accredited in accordance with federal guidelines. The system accreditation is reviewed on an annual basis utilizing the risk management framework model.
The technology incorporates web access which is role-based access. The publicly available information is separated from the agency information by firewall and network segmentation. Access to both is limited to only the roles assigned to the user.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

__✓__ Yes, the PII/BII is searchable by a personal identifier.

____ No, the PII/BII is not searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

✓	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: - COMMERCE/DEPT-5, Freedom of Information Act and Privacy Act Request Records - COMMERCE/DEPT-27, Investigation and Threat Management Records - COMMERCE/DEPT-13, Investigative and Security Records - COMMERCE/DEPT-14, Litigation, Claims, and Administrative Proceeding Records
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

✓	There is an approved record control schedule. Provide the name of the record control schedule: The record control schedule for FOIAonline is General Records Schedule 14, Information Services Records
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
✓	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	✓	Overwriting	✓
Degaussing		Deleting	✓

Other (specify):

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
✓	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.)*

✓	Identifiability	Provide explanation: Individuals can be identified by name, e-mail address, phone number, etc.
✓	Quantity of PII	Provide explanation: As collection includes a variety of information that is reflective of all DOC FOIA requests and responses entered by requesters or FOIA Specialists, there is a significant amount of information that the system maintains.
✓	Data Field Sensitivity	Provide explanation: Most of the information collected and disseminated is nonsensitive, with the exception of financial information.
✓	Context of Use	Provide explanation: Requesters are required to provide a name and mailing address to make a FOIA request, which is a public request, pursuant to the Department of Commerce's FOIA regulations, 15 CFR §4.4.
✓	Obligation to Protect Confidentiality	Provide explanation: The Privacy Act of 1974, as amended (5 U.S.C. 552a) protects the personal information submitted to FOIAonline and retained in the system. The Privacy Act regulates how the government can disclose, share, provide access to, and maintain the personal information that it collects. Not all information collected in FOIAonline may he covered by the Privacy Act. Note: FOIA requesters (except those making requests for records on themselves) do not ordinarily expect that their names will be kept private and therefore, their names may be released under a FOIA request seeking the names of FOIA requesters.
	Access to and Location of PII	Provide explanation:
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

As there is a persistent potential for insider threat, all users are required to take cybersecurity and privacy awareness training. Unauthorized access or public release of PII can pose adverse impacts to the individuals affected. To mitigate this impact, information released to FOIA requesters is reviewed by releasing DOC bureau officials, DOC FOIA/Privacy officials, and system Subject Matter Experts prior to entering into FOIAonline.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
✓	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
✓	No, the conduct of this PIA does not result in any required technology changes.