Version Number: 01-2015

U.S. Department of Commerce
Office of the Secretary

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

Reviewed by: Michael Toland, Bureau Chief Privacy Officer

MICHAEL TOLAND

Digitally signed by MICHAEL TOLAND
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=MICHAEL TOLAND, 0.9.2342.19200300.100.1.1=13001000249566
Date: 2016.06.10 11:23:01 -04'00'

☑ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

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

Catrina D. Purvis

Digitally signed by Catrina D. Purvis
DN: cn=Catrina D. Purvis, o=Office of the Secretary, Office of Privacy and Open Government, ou=US Department of Commerce, email=cpurvis@doc.gov, c=US
Date: 2016.09.28 19:05:33 -04'00'

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

(a) a general description of the information in the system

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 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 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.

In order for FOIAonline to provide the above-mentioned functionality, the system stores sensitive and non-sensitive personally identifiable information (PII), business identifiable information (BII), and FOIA case-related documents and other information. For example, the system may include requester information, such as the name, address, organization, phone number, and email address of requesters; request information, such as request description, request fee category and processing track; request submitted, perfected, and acknowledgement sent dates; incoming requests and supporting information; correspondence developed during

processing of requests; initial, interim, and final determination letters; records summarizing pertinent facts about requests and action taken; copy or description of records released; and description of records denied. Records responsive to a request are released with one of the following options: unredacted, unreleasable; redacted, unreleasable; unredacted, releasable to the general public; redacted, releasable to the general public; or release to the requester only.

(b) a description of a typical transaction conducted on 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 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.

1. FOIA Transaction – entered directly into the automated system
    a. Requester starts FOIAonline session by:
        i. Initiating a Web browser, such as Internet Explorer, Google Chrome, or Mozilla Firefox.
        ii. Starting a FOIAonline session using the URL: https://foiaonline.regulations.gov/foia/action/public/home.
        iii. Note: A FOIAonline FOIA Public User Guide is available at: https://foiaonline.regulations.gov/foia/action/public/home resources, to assist requesters with using the system.
    b. Requester enters request for information in to system (requester can either log into the system or enter the information as a public user).
    c. FOIA/PA Officer or designee reviews unassigned requests.
    d. FOIA/PA Officer or designee assigns unassigned requests.
    e. FOIA Specialist or assigned office reviews request.
    f. FOIA Specialist or assigned office constructs fee estimate or searches for responsive records, based on FOIA Office instructions.
    g. If fee estimate or actual fees:
        i. Requester is notified about fees one of two ways:
            1. Via email through the FOIAonline system, if the requester has provided an email address.
            2. Via letter if the requester has not provided an email address
        ii. Requester pays or agrees to pay fees in writing by letter.
        iii. FOIA Specialist enters fee information into the FOIAonline system.
    h. After the FOIA Office requests a search to be conducted, the search for responsive records is conducted by program office(s) or agency component(s) reasonably expected to have records responsive to a FOIA request.
    i. FOIA Specialist or assigned office reviews records and redacts, as needed
    j. Responsive records, if any, are uploaded by FOIA Specialist into system (sensitive or certain Titled-protected records (records protected by statute) are not uploaded).
    k. Response letter is generated by the FOIA Specialist assigned to the request:

i. For adverse determinations (e.g., redactions, no records found, fee waiver request denied, etc.), a disclosure official, designated in the Department of Commerce's FOIA and Privacy Act regulations, 15 CFR Part 4 Appendix B, signs the response letter.
ii. For other response letters, the FOIA Specialist may be delegated by the appropriate FOIA Officer to sign the response letter.

l. FOIA Specialist uploads signed response letter into system.
m. Response letter is sent to requester:
   i. Sent via system if requester has email address.
   ii. Sent via mail if requester does not have email address.
n. FOIA Specialist closes out request in system.

2. FOIA Transaction – paper, fax, or email formation
   a. FOIA/PA Officer or designee receives request.
   b. FOIA/PA Officer assigns staff to enter request into automated system.
   c. FOIA/PA Officer or designee reviews unassigned requests.
   d. FOIA Specialist or assigned office reviews request.
   e. FOIA Specialist or assigned office constructs fee estimate or searches for responsive records, based on FOIA Office instructions.
   f. If fee estimate or actual fees:
      i. Requester is notified about fees one of two ways:
         1. Via email through the FOIAonline system, if the requester has provided an email address.
         2. Via letter if the requester has not provided an email address
      ii. Requester pays or agrees to pay fees in writing by letter.
      iii. FOIA Specialist enters fee information into the FOIAonline system.
   g. After the FOIA Office requests a search to be conducted, the search for responsive records is conducted by program office(s) or agency component(s) reasonably expected to have records responsive to a FOIA request.
   h. FOIA Specialist or assigned office reviews records and redacts, as needed.
   i. Responsive records, if any, are uploaded by FOIA Specialist into system (sensitive or certain Titled-protected records (records protected by statute) are not uploaded).
   j. Response letter is generated by the FOIA Specialist assigned to the request.
      i. For adverse determinations (e.g., redactions, no records found, fee waiver request denied, etc.), a disclosure official, designated in the Department of Commerce's FOIA and Privacy Act regulations, 15 CFR Part 4 Appendix B, signs the response letter.
      ii. For other response letters, the FOIA Specialist may be delegated by the appropriate FOIA Officer to sign the response letter.
   k. FOIA Specialist uploads signed response letter into system.
   l. Response letter is sent to requester:
      i. Sent via system if requester has email address.
      ii. Sent via mail if requester does not have email address.
   m. FOIA Specialist closes out request in system.

(c) any information sharing conducted by the system

1. 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.

2. Information shared with Federal agencies - all FOIA case information is shared with:
    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.

(d) a citation of the legal authority to collect PII and/or BII

1. PII/BII is collected pursuant to:
    a. Freedom of Information Act, 5 U.S.C. 552.
    b. Government Organization and Employees, Title 5, U.S.C.
    c. Records management by agency heads, 44 U.S.C. § 3101.
    d. Departmental regulations, 5 U.S.C. § 301.
2. PII is also collected pursuant to:
    a. Privacy Act of 1974 as amended, 5 U.S.C. 552a.

(e) the Federal Information Processing Standard (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	X	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):					

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*		e. File/Case ID	X	i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender		j. Telephone Number	X	p. Military Service	
e. Age		k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify): Fax number, requester's Organization					

Work-Related Data (WRD)					
a. Occupation		d. Telephone Number	X	g. Salary	X
b. Job Title	X	e. Email Address	X	h. Work History	
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address		d. Queries Run		f. Contents of Files	X
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	X	Online	X
Telephone		Email	X		
Other (specify):					

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

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

2.3 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):			

X	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):			

X	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			
To determine eligibility		For administering human resources programs	
For administrative matters		To promote information sharing initiatives	
For litigation	X	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): To support requirements of the Freedom of Information Act, 5 U.S.C. 552; the Privacy Act of 1974, as amended, 5 U.S.C. 552a; and the Open Government Act			

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/BII 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/BII 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/BII identified in Section 2.1 of this document is in reference to federal employees / contractors, members of the public and private entities.

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	X		X
DOC bureaus	X		X
Federal agencies	X		
State, local, tribal gov't agencies	X		
Public	X		X
Private sector	X		
Foreign governments			
Foreign entities			
Other (specify):			

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

6.2 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:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 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	X	Government Employees	X

Contractors	X		
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.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	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.regulations.gov/foia/action/public/home#privacyActPage	
	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.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Individual users can choose not to include their PII/BII 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 to the Department of Commerce's FOIA regulations, 15 CFR § 4.4.
	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.

X	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. Individual users can choose not to include their PII/BII. However, if individuals decide not to provide the required information, their requests cannot be entered into the system or processed.
	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.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: The system requires individuals to review their PII/BII 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 and/or BII.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

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.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: All activity within the system is tracked by an automated audit log.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): December 11, 2015 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	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 (POAM).
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
X	Other (specify): All nonpublic users are subject to a Code of Conduct that includes the requirement for confidentiality. Staff with access to PII/BII 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.

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 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."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: COMMERCE/DEPT-5, Freedom of Information Act and Privacy Act Request Records
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, a SORN is not being created.

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.)*

X	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:
X	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	X	Overwriting	X
Degaussing		Deleting	X
Other (specify):			

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

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.

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
X	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 levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: The ability to identify specific individuals has been evaluated.
X	Quantity of PII	Provide explanation: The collection contains all of the Departmental FOIA requests and responses based on the information entered by requesters and/or FOIA Specialists.
X	Data Field Sensitivity	Provide explanation: The collection of name, home/business address, home/business telephone number, home/business email address, and organization.
X	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.
X	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 be 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 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:
X	No, the conduct of this PIA does not result in any required business process changes.

12.2 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:
X	No, the conduct of this PIA does not result in any required technology changes.